Excuse me, do you speak ITGC?

Drs. P.J. Mancham RE RA, drs. M.A. Ringia en drs. E.P. Rutkens RE

Vanaf 2005 zijn alle beursgenoteerde ondernemingen in de EU verplicht IFRS toe te passen. Met deze verplichting is een belangrijke stap gezet in de wereldwijde harmonisatie in de financiële verslaggeving ofwel de 'financiële wereldtaal'. Als we kijken naar het beheersingsvraagstuk binnen het IT-domein zijn er momenteel diverse standaarden voorhanden, echter ontbreekt een 'wereldtaal'. Ondanks dat de IT general controls door de IT-auditberoepsgroep (internationaal) zijn uitgewerkt, blijkt in de praktijk dat verschillende belanghebbenden (zoals klanten, toezichthouders en de externe accountant) verschillende standaarden gebruiken dan wel verschillende verklaringen vragen over de beheersing van de IT controls. Dit leidt nogal eens tot afstemmingsproblemen en interpretatieverschillen. Dit artikel geeft een aanzet om de IT controls zowel intern als extern, nationaal en internationaal te harmoniseren en standaardiseren.

Inleiding

Een aantal ontwikkelingen in de afgelopen jaren, zoals de invoering van de Sarbanes-Oxley (SOX) regelgeving en de International Financial Reporting Standards (IFRS), hebben gevolgen gehad voor de normering die de grondslag vormt voor de oordelen van auditors. Deze ontwikkelingen hebben ervoor gezorgd dat er op internationaal niveau wordt gesproken over uniformering dan wel harmonisatie van normen. Zo zijn vanuit de SOX-wetgeving heldere richtlijnen opgesteld over de verklaringen die moeten worden afgegeven door het management van een organisatie en de externe auditors. Hierbij is het van groot belang dat de onderliggende normeringen die internationaal door auditors worden gebruikt, gelijk zijn. Met andere woorden, auditors maar ook de auditees en de afnemers van de oordelen van auditors moeten dezelfde 'taal' spreken (of op z'n minst de gesproken 'taal' begrijpen). Kijken we naar de financiële verslaggeving dan zien we dat hier sinds de invoering van IFRS internationaal een set van afspraken geldt over hoe bedrijven hun jaarverslag moeten presenteren. Dat het gebruik van een dergelijk gemeenschappelijk normenkader voordelen heeft spreekt voor zich. Interpretatieverschillen worden hiermee geminimaliseerd en in bepaalde gevallen voorkomen. De accountants onder ons weten overigens wel dat er door de toepassing van IFRS als verslaggevingsstandaard in Nederland naast de Nederlandse wet- en regelgeving nog niet helemaal sprake van een eenduidige en uniforme verslaggevingstaal.

Het inrichten en onderhouden van beheersingsmaatregelen rond informatietechnologie (IT controls) is

Drs. P.J. Mancham RE RA
is als Manager van Cordares Risk & Audit Services verantwoordelijk voor de Internal Audit-functie en Risk Control-functie binnen Cordares. Hij heeft ruim zeventien jaar (Financial & IT) auditervaring opgedaan bij onder meer KPMG en Deloitte.

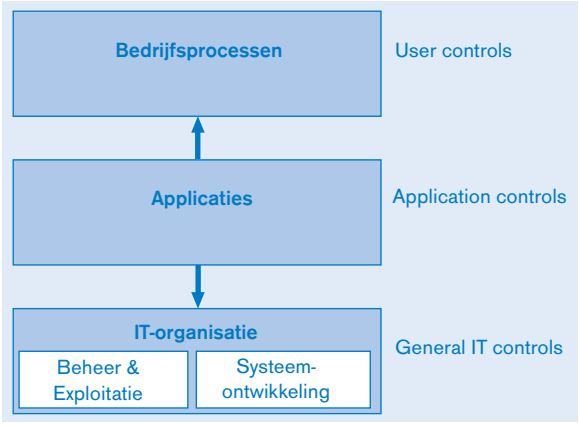
p.mancham@cordares.nl

Drs. M.A. Ringia
is werkzaam als IT-auditor bij Cordares Risk & Audit Services. Hij is daar verantwoordelijk voor de jaarlijkse IT-audits voor de SAS 70-trajecten en voor die in het kader van de controle van de jaarrekeningen. Daarnaast is hij als trekker verantwoordelijk voor de service-line Project Risk Management.

m.ringia@cordares.nl

Drs. E.P. Rutkens RE
is werkzaam als Manager bij KPMG Information Risk Management. Hij houdt zich bezig met de dienstverlening van KPMG met betrekking tot Information Security. Verder is hij betrokken bij de ontwikkeling van producten op dit gebied, waaronder beveiligingsarchitecturen en risicoanalyse.

rutkens.erik@kpmg.nl



Figuur 1. Relatie tussen application controls en IT general controls.

de afgelopen jaren, ook als onderdeel van de financiële verslaglegging en de verantwoording die daarover moet worden afgelegd, belangrijker geworden. IT controls vormen een onderdeel van de algemene interne beheersingsmaatregelen die een organisatie kan treffen. Interne beheersing definiëren we hierbij als een stelsel van processen dat is ingericht door de leiding van een organisatie om een redelijke mate van zekerheid te krijgen over het realiseren van de effectiviteit en efficiency van de bedrijfsvoering, de betrouwbaarheid van de financiële verslaglegging en de naleving van relevante wet- en regelgeving ([Fijn05]).

Bij de IT controls maken we onderscheid tussen applicatiespecifieke beheersingsmaatregelen (application controls) en algemene IT-beheersingsmaatregelen (IT general controls). De application controls omvatten alle maatregelen in en rond een specifieke toepassing.[1] De IT general controls (ITGC) hebben niet slechts betrekking op een enkele applicatie, maar op alle aspecten van de informatievoorziening.

In de publicatie *IT control Objectives for Sarbanes-Oxley* van het IT Governance Institute worden de ITGC als volgt ingedeeld:
- Access to Programs and Data (Logische toegangsbeveiliging);
- Computer operations (IT-beheer en exploitatie);
- Program changes (Wijzigingsbeheer);
- Program development (Systeemontwikkeling).

In dezelfde publicatie worden de application controls gerelateerd aan de bedrijfsprocessen en wordt een voorbeeld gegeven van application controls die de juistheid en volledigheid van de informatie in een inkoopproces kunnen waarborgen. Als we kijken naar de application controls dan heeft hier nog geen uniformering dan wel harmonisatie plaatsgevonden.

Als we kijken naar de ITGC, een belangrijk auditdomein van de IT-auditor, dan kunnen we stellen dat er steeds meer sprake is van uniformering dan wel harmonisatie: er zijn diverse normen, richtlijnen en 'best practices' die door de IT-auditor worden gehanteerd als referentiekader zoals Cobit, de Code voor Informatiebeveiliging (ISO/IEC 17799:2005), en ITIL. Op dit moment zien we dat internationaal de 'IT Control Objectives for Sarbanes-Oxley' steeds vaker als 'leidraad' door IT-auditors maar vooral door organisaties zelf worden gebruikt. De uitwerking van ITGC die in deze publicatie zijn opgenomen, zijn afgeleid van Cobit, de Code voor Informatiebeveiliging en ITIL, en sluiten aan bij COSO.

In de huidige praktijk worden er diverse internationale standaarden, zoals Cobit en de Code voor Informatiebeveiliging, gebruikt voor het beoordelen van (de onderdelen van) de IT controls, terwijl veel organisaties en ook samenwerkingsverbanden tussen organisaties ook eigen normenkaders hebben ontwikkeld, weliswaar vaak gebaseerd op algemene standaarden maar gericht op specifieke doeleinden. Door het ontbreken van een algemene standaard (een wereldtaal), die voor de meest voorkomende praktijksituaties concreet toepasbaar is, ontstaan er afstemmingsproblemen tussen organisaties en auditors bij het onderling gebruikmaken van verklaringen over de beheersing van de IT controls.

In dit artikel wordt eerst een aantal ontwikkelingen geschetst die aanleiding geven om te komen tot verdere harmonisatie en standaardisatie van IT controls. Alvorens, naar analogie van de ontwikkeling van IFRS, de weg naar een IT controls wereldtaal te verkennen, worden de voor de IT controls relevante raamwerken en standaarden benoemd. Daarnaast wordt een overzicht gegeven van verklaringen die momenteel door organisaties worden gebruikt om aan derden aan te tonen of en zo ja, in hoeverre de IT controls 'in control' zijn.

Ontwikkelingen

IT is bij nagenoeg alle ondernemingen een belangrijk onderdeel van de bedrijfsprocessen en is feitelijk het 'hart' van de organisatie. Organisaties steunen dan primair op de kwaliteit van de IT controls om de betrouwbaarheid van de (financiële) gegevensverwerking te waarborgen. Mede als gevolg van de steeds toenemende

1) Kenmerk van een application control is dat de beheersingsmaatregelen in de programmatuur zijn vastgelegd, zodat ze consequent worden uitgevoerd. Soms komen bij application controls uitgebreide berekeningen voor, maar vaak ook blijven application controls beperkt tot vergelijkingen. Bij berekeningen kan gedacht worden aan eenvoudige controlegetallen of complexe hashtotals en bij vergelijkingen aan totalen of standen of aan details in een transactie ([Fijn06]).

Kader 1. Sarbanes-Oxley (SOX).

SOX

De Amerikaanse SOX-regelgeving uit 2002 is genoemd naar de opstellers ervan, de voorzitters van het Huis van Afgevaardigden en de Senaat van de Verenigde Staten, Sarbanes en Oxley. De prikkel voor deze wetgeving komt voort uit de debacles die aan het eind van de vorige eeuw bij een aantal bedrijven ontstonden. Daarbij speelden 'oneerlijkheid' en 'ondoorzichtigheid' in het handelen van de bedrijfsleiding een belangrijke rol. De SOX-wetgeving richt zich op de inrichting van bedrijfsprocessen met betrekking tot de financiële verslaglegging en de verantwoording die daarover moet worden afgelegd. *Bron: Trends in IT-beveiliging 2006.*

afhankelijkheid van IT zien we een aantal ontwikkelingen die aanleiding geven om te komen tot verdere harmonisatie van IT controls. Een voorbeeld is de steeds verdergaande proces- en ketenintegratie. Om de efficiency in het auditen van dergelijke informatieketens te bevorderen zien we auditors steeds vaker verklaringen afgeven waarop een andere auditor kan steunen. Het bekendste voorbeeld hiervan is een zogeheten SAS 70-verklaring.

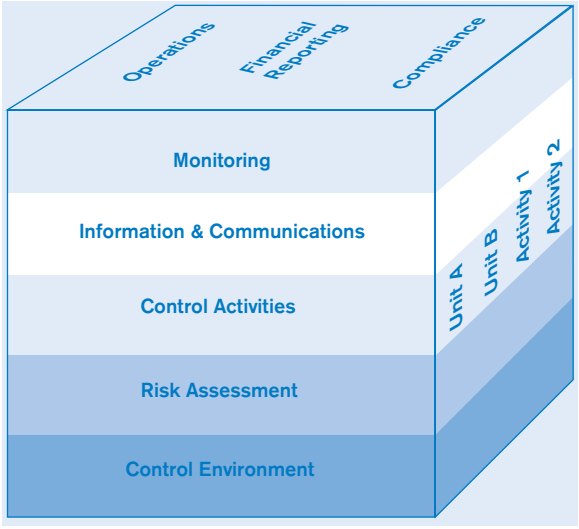
Daarnaast zien we dat door de ketenpartners en auditors meer en meer gebruik zal worden gemaakt van een gemeenschappelijk dan wel geïntegreerd en procesgericht stelsel van internecontrolemaatregelen. Nu zien we vaak dat interne beheersingssystemen van de verschillende ketenpartners onvoldoende op elkaar aansluiten en hanteren de betrokken (externe) auditors hun eigen normenkader. Niet alleen vertoont het werk van de auditors hierdoor overlap, maar tevens bestaat de kans dat er onvoldoende inzicht is in de kwaliteit van het gehele proces.

Bovengenoemde ontwikkelingen hebben een belangrijke impact op de wijze waarop de IT-auditor zijn of haar werkzaamheden uitvoert en vastlegt. De verschuiving van 'trust me' naar 'prove me', het toenemende belang van transparantie en de aard van de 'in control'-verklaringen van het management eisen dat de IT-auditor te allen tijde de deugdelijke grondslag van de uitgevoerde audit dient aan te tonen. Dit betekent niet alleen standaardisatie van werkwijze (waaronder dossiervorming) maar ook standaardisatie van normenkaders. In de volgende paragraaf wordt een overzicht gegeven van de raamwerken en standaarden die gebruikt worden voor IT controls. Hierna gaan we in op een aantal verklaringen die door organisaties worden gebruikt om aan derden aan te tonen of en zo ja, in hoeverre de ITGC 'in control' zijn.

Raamwerken en standaarden voor IT controls

In de inleiding hebben we al aangegeven dat er rond het gebied van de application controls nauwelijks sprake is van harmonisatie en uniformering. Er zijn dan ook geen breed toepasbare normenkaders, richtlijnen en/of 'best practices'.

Voor het inrichten en onderhouden van de ITGC zien we in de praktijk dat verschillende raamwerken en standaarden worden gehanteerd. Hieronder geven we een kort overzicht van de verschillende raamwerken/standaarden. Het algemeen aanvaarde COSO-model voor interne beheersing kan worden gezien als de basis voor al deze raamwerken en wordt daarom als eerste behandeld. Daarna besteden we aandacht aan Cobit, een raamwerk voor de beheersing van informatietechnologie, dat mede op COSO is gebaseerd. Andere relevante raamwerken dan wel standaarden die we hier behandelen zijn de



Figuur 2. COSO.

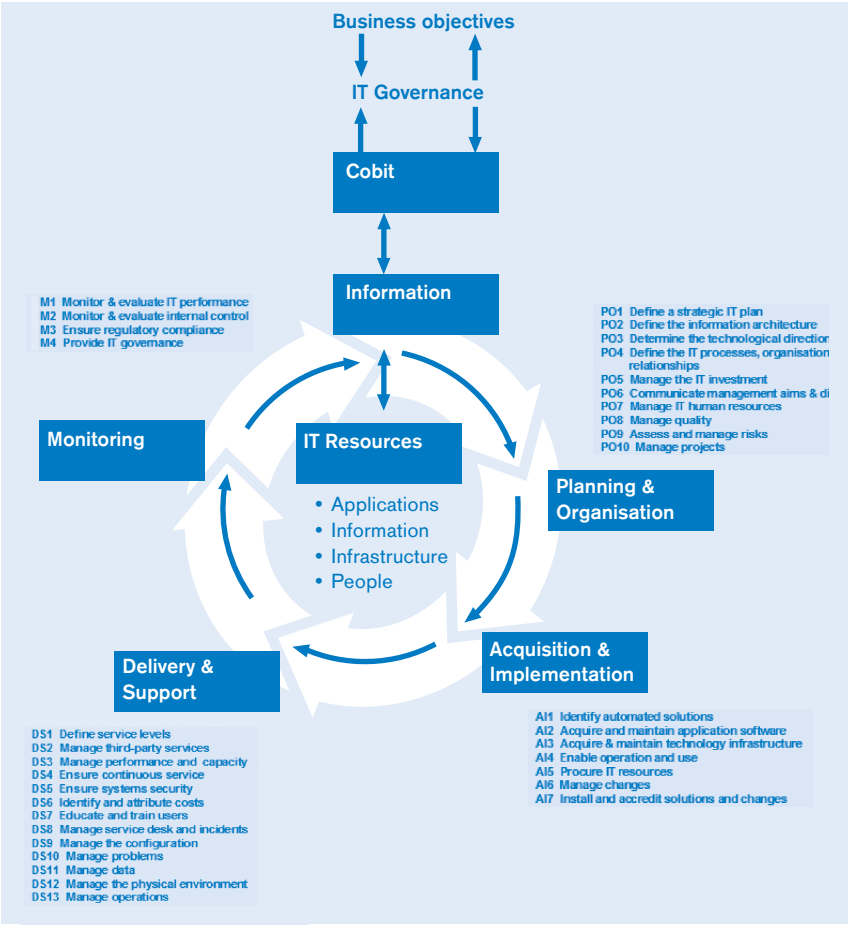
Code voor Informatiebeveiliging (ISO/IEC 17799:2005) en ITIL voor IT-beheer (ISO/IEC 20000:2005). Deze raamwerken, die elkaar gedeeltelijk overlappen, geven een verdere verdieping van de aandachtsgebieden binnen Cobit.

COSO

COSO heeft niet zozeer betrekking op IT, als wel op interne beheersing in brede zin. Als geïntegreerd raamwerk voor corporate governance wordt meestal gesteund op het COSO-model. Dit model is in de jaren negentig ontwikkeld door de Committee of Sponsoring Organizations of the Treadway Commission als gevolg van een aantal boekhoudschandalen in de Verenigde Staten. Het COSO-model helpt ondernemingen en andere organisaties met het beoordelen en verbeteren van de interne beheersingssystemen. Volgens COSO bestaat interne beheersing uit vijf verschillende componenten die onderling samenhangen: beheersingsomgeving, risicoanalyse, beheersingsmaatregelen, informatie en communicatie, en monitoring.

Cobit

Eind jaren negentig ontwikkelde de Information Systems Audit and Control Association (ISACA) de Control Objectives for Information and related Technology, ofwel Cobit. Cobit wordt gezien als de invulling van het COSO-model voor IT. Het Cobit-raamwerk biedt management en auditors richtlijnen om de IT-beheerprocessen in te richten en te beoordelen. Het Cobit-raamwerk is gebaseerd op drie dimensies. De eerste dimensie bestaat uit een zevental kwaliteitskenmerken van informatie en informatiesystemen: effectiviteit, efficiency, vertrouwelijkheid, integriteit, beschikbaarheid, naleving en betrouwbaarheid. De tweede dimensie bestaat uit vijf categorieën van informatiemiddelen: gegevens, applicatiesystemen, technologie, faciliteiten en mensen. De derde dimensie bestaat uit vier domeinen, waarbinnen beheersingsmaatregelen worden gegroepeerd: de



Figuur 3. Cobit.

planning en organisatie van de inzet van informatietechnologie, de acquisitie en implementatie van informatiesystemen, de levering van IT-diensten en de ondersteuning daarbij, en de bewaking van de voorgaande drie domeinen. Binnen elk van de domeinen definieert Cobit een aantal beheersingsdoelstellingen op procesniveau. In totaal zijn er 34 van dergelijke doelstellingen.

Code voor Informatiebeveiliging

De Code voor Informatiebeveiliging is een 'best practice' voor het inrichten van een beveiligingsproces en het invoeren van beveiligingsmaatregelen. De Code voor Informatiebeveiliging is uitgegroeid tot de internationaal meest gebruikte (toonaangevende) standaard op het gebied van informatiebeveiliging.

De Code beschrijft meer dan honderd beveiligingsmaatregelen die door de opstellers ervan als minimaal noodzakelijk worden beschouwd. De maatregelen zijn ingedeeld in elf hoofdstukken, die gaan over beleid, organisatie, classificatie, personeel, fysieke beveiliging, beheer, logische toegangsbeveiliging, ontwikkeling en onderhoud, beveiligingsincidenten, continuïteit en naleving (compliance).

ITIL

Een andere relevante standaard is de Information Technology Infrastructure Library (ITIL), een verzameling richtlijnen voor het beheer van informatiesystemen, opgesplitst in modules voor de meest uiteenlopende beheerprocessen: configuratiebeheer, wijzigingsbeheer, probleembeheer, netwerkbeheer, enz. ITIL is een 'best practice': de procesbeschrijvingen zijn gebaseerd op de manier waarop een groot aantal bedrijven en instellingen het beheer van de informatievoorziening heeft ingericht. ITIL is inmiddels algemeen geaccepteerd en wordt in tal van varianten toegepast. Aan ITIL is twee jaar geleden een belangrijke ontbrekende schakel toegevoegd: de module Security Management, een Nederlands initiatief, gebaseerd op de Code voor Informatiebeveiliging. Veel automatiseringsafdelingen en serviceorganisaties werken op dit moment volgens ITIL.

In 2005 verscheen ISO/IEC 20000, een standaard voor IT Service Management. Deze standaard kent twee delen, namelijk 20000-1, waarin de formele specificaties voor certificatie staan beschreven, en 20000-2, 'best practice' voor IT Service Management. ISO/IEC 20000 is gebaseerd op BS 15000.

Verklaringen of statements over de beheersing van IT controls

Niet alleen SOX-trajecten, maar ook de eis van opdrachtgevers om de kwaliteit van uitbestede diensten te beheersen leidt tot de vraag naar SAS 70-verklaringen en/of andere verklaringen. Daarnaast eisen sommige instellingen van hun leveranciers dat ze aan een algemeen erkende norm voldoen zoals de Code voor Informatiebeveiliging. Soms wordt in aanvulling hierop nog een oordeel gevraagd met betrekking tot een specifiek stuk dienstverlening voor een bepaalde leverancier in de vorm van een third-partymededeling (TPM).

Hierna volgt een kort overzicht van een aantal verklaringen of statements over de beheersing van de IT controls. Deze verklaringen verstrekken een bepaalde mate van zekerheid. Per type verklaring staan we dan ook kort stil bij het zekerheidsniveau van de betreffende verklaring.

TPM

Een third-partymededeling (TPM) is een schriftelijke uiting van een onafhankelijk auditor ten behoeve van één of meer gebruikers waarbij naar aanleiding van een onderzoek een bepaalde mate van zekerheid wordt geboden over het stelsel van beheersingsmaatregelen dat de kwaliteit van de dienstverlening van een leverancier moet waarborgen. Afhankelijk van het type van onderzoek geeft een TPM een redelijke (audit) of beperkte (review) mate van zekerheid.[2] De wijze waarop

2) Met *redelijke mate van zekerheid* bedoelen we de situatie waarin de IT-auditor toereikend bewijsmateriaal heeft verkregen om te kunnen oordelen dat het object van onderzoek in alle van materieel belang zijnde opzichten voldoet aan de gestelde criteria. Met *beperkte mate van zekerheid* bedoelen we de situatie waarin de IT-auditor toereikend bewijsmateriaal heeft verkregen om ervan overtuigd te zijn dat het object van onderzoek gegeven de omstandigheden voldoet aan de criteria. De mate van zekerheid correspondeert met 'plausibel'.

het onderzoek wordt uitgevoerd en de wijze waarop wordt gerapporteerd, is niet aan bepaalde regels gebonden zoals bij SAS 70.

SAS 70-verklaring

SAS 70 staat voor Statement on Auditing Standards No. 70. Met SAS 70 wordt de standaard aangeduid van het rapport waarmee de ene auditor zich richt tot de andere auditor. De externe auditor van de aanbieder (service auditor) beoordeelt de interne beheersings- en controlemaatregelen die relevant zijn voor een klant en geeft hierover een oordeel af. De externe auditor van de klant (user auditor) kan vervolgens steunen op dit oordeel.
De serviceorganisatie (bijvoorbeeld IT service provider) beschrijft in een SAS 70-rapport op hoofdlijnen de beheerorganisatie en geeft hierbij aan hoe zij specifieke beheersingsdoelstellingen bereikt. Een externe auditor voegt een rapport toe over de mate waarin die beheersingsdoelstellingen worden gerealiseerd. Het resultaat is dat de uitbestedende organisatie inzicht krijgt in de wijze waarop de uitbestede processen worden beheerst.

Een SAS 70-verklaring geeft een redelijke mate van zekerheid dat de beheersingsmaatregelen op een bepaald moment in opzet toereikend zijn en ook daadwerkelijk bestaan (type I-verklaring) dan wel in een bepaalde periode ook hebben gewerkt (type II-verklaring).

Hoewel SAS 70 een aantal formaliteiten kent – zoals de verplichte hoofdstukindeling – zijn de grenzen van het object van onderzoek van een SAS 70-rapport niet voorgeschreven. De serviceorganisatie en de uitbestedende organisatie zijn (in onderling overleg) vrij om te bepalen welke processen en beheersingsdoelstellingen worden meegenomen in het onderzoek.

Certificatie van Informatiebeveiliging op basis van ISO/IEC 27001 en van IT Service Management op basis van ISO/IEC 20000

Certificering van Informatiebeveiliging of IT Service Management zijn onderzoeken waarbij een geaccrediteerde certificerende instelling niet zozeer de beheersingsmaatregelen op zich beoordeelt, maar het proces dat is ingericht om de (met behulp van risicoanalyse) geselecteerde beheersingsmaatregelen vast te stellen, in te voeren, uit te voeren, te controleren, te beoordelen en te verbeteren. De organisatie dient zelf aan te tonen dat het proces functioneert in overeenstemming met de ISO-standaard. In feite worden de geselecteerde beheersingsmaatregelen door de auditor aan de hand van steekproeven getoetst om het functioneren van het proces te beoordelen. Een certificeringsonderzoek kent grofweg twee fasen. De documentatiereview (te vergelijken met opzet), waarin de risicobeoordeling, de selectie van risicoreducerende maatregelen en de documentatie wordt getoetst, en de implementatiebeoordeling (te vergelijken met bestaan), waarin het stelsel van

Figuur 4. SAS 70.

beheersingsmaatregelen wordt beoordeeld. Komt een organisatie in aanmerking voor een certificaat dan is dit certificaat voor drie jaar geldig. Gedurende deze periode voert de auditor periodieke controles uit om vast te stellen of het gedocumenteerde proces blijvend voldoet aan de ISO-standaard. Een dergelijk certificaat geeft een beperkte mate van zekerheid, ofwel de auditor heeft een gerechtvaardigd vertrouwen dat het gedocumenteerde proces functioneert in overeenstemming met de ISO-standaard.

Andere verklaringen

Naast de hierboven genoemde verklaringen zijn er nog een aantal andere verklaringen die in de praktijk voorkomen om bijvoorbeeld het vertrouwen van consumenten in websites te vergroten, zoals Systrust/Webtrust (www.webtrust.org). Met een Systrust- of een Webtrust-rapport geeft een onafhankelijke accountant aan in hoeverre de verklaring van het management dat de beheersingsmaatregelen in overstemming zijn met de van toepassing zijnde Trust Service Principles van de AICPA, redelijk en gerechtvaardigd is. De Trust Service Principles betreffen Security, Avalability, Processing Integrity, Online Privacy en/of Confidentiality. Een Systrust- of Webtrust-rapport geeft een beperkte mate van zekerheid.

De verschillende verklaringen die we hebben behandeld, zijn moeilijk met elkaar te vergelijken. Niet alleen omdat de reikwijdte en het onderzoeksobject verschillend zijn, maar ook omdat er geen voorgeschreven normen zijn voor de IT controls.

Een ITGC wereldtaal à la IFRS

Het nut van een ITGC-normenset en de weg ernaartoe

In de praktijk is het voor organisaties lastig om, naar tevredenheid van de verschillende belanghebbenden (auditor, toezichthouders, klant, etc.), een uitspraak te doen over het al dan niet 'in control' zijn. Dit komt niet zozeer doordat de (IT-) organisaties dit niet willen of kunnen, integendeel. De complexiteit zit vooral in het feit dat belanghebbenden nogal eens een verschillende uitspraak vragen en/of verschillende normenkaders hanteren. Binnen de eigen organisatie werkt de IT-afdeling vaak conform ITIL, terwijl vanuit oogpunt van interne beheersing door de business gekozen is voor Cobit, een bepaalde klant eist een certificaat op basis van ISO/IEC 27001:2005 en weer een andere klant vraagt een SAS 70-verklaring. En dan hebben we de externe accountant

Als het gaat om de beheersing van IT controls spreken de verschillende belanghebbenden nog onvoldoende dezelfde taal

en toezichthouder nog niet eens genoemd. Om een lang verhaal kort te maken: als het gaat om de beheersing van de IT controls spreken de verschillende belanghebbenden nog onvoldoende dezelfde taal. Een gemeenschappelijke taal levert niet alleen voordelen op in de interne en externe communicatie maar ook worden er besparingen gerealiseerd in de kosten voor de IT-beheersing als geheel. De weg naar een dergelijke gemeenschappelijke ITGC-taal kan lopen zoals het is gegaan met IFRS als wereldwijde financiële taal.

IFRS als voorbeeld hoe het kan

In de afgelopen jaren moesten de beursgenoteerde bedrijven overgaan naar een wereldwijde financiële verslaggevingstaal: IFRS. De Europese Commissie heeft in een verordening vastgelegd dat alle beursgenoteerde bedrijven vanaf 1 januari 2005 hun jaarverslag in overeenstemming met IFRS moeten presenteren. IFRS is opgesteld door de International Accounting Standards Board (IASB). De IASB is een onafhankelijk internationaal orgaan belast met het opzetten van standaarden voor jaarverslagen en jaarrekeningen. De IASB bestaat niet alleen auditors, maar ook uit bedrijven (opstellers van jaarverslagen) en bijvoorbeeld overheden (gebruikers van jaarverslagen).

Eén van de belangrijkste doelstellingen van IFRS is de transparantie en onderlinge vergelijkbaarheid tussen ondernemingen te verbeteren. Met de invoering van IFRS is tevens de onderliggende normering voor financiële verslaggeving geharmoniseerd. Wereldwijd heeft

Praktijk bij Cordares

Cordares is uitvoerder van pensioenregelingen voor ondernemingen en bedrijfstakken en van andere arbeidsvoorwaardelijke regelingen, collectief en privaat. Daarnaast verzorgt Cordares aanvullende inkomensverzekeringen en dekt het werkgeversrisico's af. De meer dan één miljoen deelnemers mogen rekenen op een uitgebalanceerd pakket voor inkomenszekerheid. Bij pensionering, maar ook bijvoorbeeld bij arbeidsongeschiktheid of overlijden. Momenteel voert Cordares 27 verschillende regelingen uit met een totaal van één miljard euro aan premie-inkomsten per jaar. Het belegd vermogen bedraagt 23 miljard euro.

Cordares IT levert IT-diensten aan zowel interne partijen als aan externe partijen zoals het UWV. Voor het UWV wordt jaarlijks een TPM verstrekt door de stafafdeling Risk & Audit Services (RAS). Deze TPM is gebaseerd op door het UWV aangeleverde normen en is gericht op opzet, bestaan en werking van de (Key) IT controls.

Naast de jaarlijkse TPM worden IT-auditwerkzaamheden door RAS uitgevoerd voor de verschillende SAS 70-trajecten (type I en type II), voor het verantwoordelijk lijnmanagement, voor de controle van de jaarrekeningen van de klanten van Cordares en de jaarrekeningen van Cordares zelf. Bij deze IT-auditwerkzaamheden werd tot 2006 gebruikgemaakt van verschillende ITGC-normensets afkomstig uit verschillende bronnen. Ook de diepgang van de IT-audits was per onderzoek verschillend.

In 2006 is het stelsel van informatiebeveiliging van Cordares IT gecertificeerd op basis van ISO 27001 (voorheen BS 7799-2) door BSI Management B.V.

In 2005 is Cordares gestart met de code-Tabaksblat. Deze code heeft zijn weerslag op de beoordeling en beheersing van de IT-risico's in het kader van de jaarlijkse 'In Control Statements'.

Als recente relevante ontwikkeling in dit kader valt IT2Share te noemen; het samenwerkingsverband van Cordares en Mn Services op het gebied van continuïteit. Bij IT2Share hebben de auditors van RAS te maken met normen van Cordares, Mn Services en van de controlerende accountants van beide organisaties.

Deze ontwikkelingen waren voor RAS aanleiding om 'het roer om te gooien', om meer vanuit een 'multi purpose single audit'-gedachte te gaan werken.

RAS heeft in 2006 een ITGC-normenset ontwikkeld die de basis vormt voor de IT-audits binnen Cordares. Deze set is dekkend voor bovenstaande onderzoeken. Binnen de normenset maakt RAS onderscheid tussen de Key IT Controls en de zogenaamde Add On Controls die in bijzondere onderzoeken worden meegenomen. De ITGC-normenset is in een vroeg stadium ook afgestemd met verantwoordelijk management en de externe accountants. Het verantwoordelijk IT-management heeft eind 2006 de ITGC-normenset opgepakt om deze verder te integreren in de IT-processen binnen Cordares. Hiervoor is een project opgestart dat medio 2007 dient te worden afgerond. De IT-organisatie wil zelf vanuit een zelflerende gedachte excelleren om in continuïteit aantoonbaar 'in control' te zijn.

Na het afronden van de ITGC-audits 2006 zal RAS in het voorjaar van 2007 de gekozen aanpak, gehanteerde werkwijze en toegevoegde waarde van de nieuwe aanpak kritisch evalueren en waar nodig actualiseren. De externe accountants worden bij deze evaluatie nauw betrokken.

Kader 2. Praktijkcasus Cordares.

de toepassing van IFRS ook voor de auditors voordelen bij het uitvoeren van financial audits. Immers, overal ter wereld wordt gebruikgemaakt van dezelfde normeringen op het gebied van financiële verslaggeving. Een kritische lezer zal bij het lezen van deze passage opmerken dat IFRS nog niet wereldwijd verplicht is voor alle ondernemingen en dat het 'principle based' (naar de geest) is en niet 'rule based' (naar de letter)[3]. Dat is zeker zo, maar de invoering van IFRS heeft de weg naar volledige harmonisatie versneld. IFRS heeft aangetoond dat harmonisatie duidelijk voordelen heeft voor zowel de ondernemingen als de auditors.

De weg naar een IT controls wereldtaal

Om de in dit artikel geschetste problematiek het hoofd te bieden heeft een aantal grote organisaties in Nederland gezamenlijk een ITGC-raamwerk ontwikkeld. Daarnaast hebben Platform Informatiebeveiliging[4] en NOREA (de beroepsorganisatie van IT-auditors) een werkgroep in het leven geroepen, met ruime vertegenwoordiging uit de grote accountantskantoren, overheid en ICT-dienstverleners, om een algemeen aanvaarde standaard voor de ITGC te ontwikkelen. Dit alleen is echter niet genoeg. Analoog met IFRS zou een onafhankelijke en door alle belanghebbenden geaccepteerde organisatie een dergelijke standaard moeten vaststellen. Via wet- en regelgeving kan dan vervolgens het gebruik van deze standaard worden afgedwongen.

Conclusie

Binnen het IT domein neemt naar aanleiding van de ontwikkelingen in de financiële verslaggeving de aandacht voor het vraagstuk van interne beheersing in een snel tempo toe. Het nut en de noodzaak om te komen tot een geharmoniseerde normenset voor de beheersing en de beoordeling van de IT controls is in dit artikel nader toegelicht.

Als we kijken naar de application controls dan heeft hier nog geen standaardisatie dan wel harmonisatie plaatsgevonden. Nu is dit ook lastig doordat bedrijfsprocessen en dus ook de applications control per bedrijf nogal verschillen. Toch zijn er mogelijkheden voor harmonisatie en standaardisatie, bijvoorbeeld als het gaat om de wijze waarop de application controls worden bepaald. Maar daarnaast zijn er ook mogelijkheden om (analoog aan Starreveld) per typologie van organisaties voor de hand liggende application controls te definiëren.

Om te komen tot een uniforme ITGC-taal dient een onafhankelijke en breed geaccepteerde instantie een standaard vast te stellen

Kijken we naar de ITGC, dan zien we dat er verschillende standaarden, richtlijnen en 'best practices' zijn. Echter, een algemene standaard (een wereldtaal), die voor de meest voorkomende praktijksituaties concreet toepasbaar is, ontbreekt. Om te komen tot een wereldtaal is het, net als bij IFRS, van belang dat een onafhankelijke instantie die door bedrijven, overheid en auditors wordt geaccepteerd, een dergelijke standaard vaststelt.

3) *Principle based* wil zeggen dat de verslaggevingsregels gebaseerd zijn op beginselen (doelstellingen) in plaats van op gedetailleerde regels. *Rule based* verslaggevingsregels zijn erop gericht zoveel mogelijk situaties met specifieke voorschriften af te dekken.

4) Het Platform Informatiebeveiliging, kortweg PI genoemd, is een vereniging die zich beijvert voor de beveiliging van informatie en informatiesystemen. De belangrijkste pijler voor PI is het ontwikkelen en onderhouden van richtlijnen voor de praktische inrichting van informatiebeveiliging.

Literatuur

[Eijk03] S. van der Eijk-Van Eck en K.H.G.J.M. Ho RE RA, *Third-partymededelingen: de ervaringen van de gebruikersorganisaties*, Compact 2003/3.

[Fijn05] R. Fijneman, E. Roos Lindgreen en P. Veltman, *Grondslagen IT-auditing*, Sdu Uitgevers, 2005.

[Fijn06] R. Fijneman, E. Roos Lindgreen en K. Hang Ho, *IT-auditing en de praktijk*, Sdu Uitgevers, 2006.

[ITGI04] IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, 2004.

[NORE03] NOREA, *Handreiking Oordelen van gekwalificeerde IT-auditors*, 2003.

[NORE04] NOREA, *IT-Governance, Een verkenning*, NOREA, 2004.

[NORE06] NOREA, *Het profiel van de audit. Update on ICT en controle*, NOREA / Uitgeverij de kleine Uil, 2006.

[PI06] Platform Informatiebeveiliging, *Trends in IT-beveiliging 2006*, onder redactie van Cees Coumou, Hans Kroeze en Kees van der Zwan, 2006.

[Roos02] E. Roos Lindgreen, *Over informatiebeveiliging, accountancy, informatiebeveiliging*, Rede uitgesproken bij de aanvaarding van het ambt van hoogleraar IT en Auditing aan de Universiteit van Amsterdam op woensdag 16 oktober 2002.

[Rutk06] E.P. Rutkens en B. Derksen, *Trends in IT en IT-auditing*, Compact 2006/1.