Information risk management en Audit 2000

R.A. Jonker RA

In dit artikel wordt ingegaan op de integratie van Information Risk Management[1] (IRM)-diensten in KPMG's vernieuwde controleaanpak. Deze controleaanpak wordt onder de naam Audit 2000 sinds 1997 gefaseerd wereldwijd ingevoerd. De diensten die in dit verband de revue passeren zijn: IT Controls Benchmark, World Class IT en Business Process Analysis.

1) In dit artikel is ervoor gekozen de in Nederland gebruikelijke aanduiding EDP-auditing te vervangen door de internationaal binnen KPMG gebruikelijker aanduiding Information Risk Management.

Inleiding

De hedendaagse accountantscontrolemethodiek van de Big Five-kantoren is gebaseerd op risicoanalyse. De op risicoanalyse gebaseerde – internationaal gestandaardiseerde – controleaanpak van KPMG werd in 1994 vastgelegd in het handboek KPMG Audit Services (KAS, [KPMG94]). KAS laat er geen misverstand over bestaan dat een effectieve en efficiënte accountantscontrole alleen mogelijk is als de auditor een grondige kennis heeft van het bedrijf en de bedrijfsomgeving van zijn cliënt. Alleen zo is hij in staat zich een oordeel te vormen over belangrijke beweringen in de jaarrekening. Beweringen die tot uitdrukking komen in de waardering van posten op de balans en in de resultatenrekening en die niet zelden de resultante zijn van complexe economische transacties of relaties.

KAS geeft primair aan *wat* de auditor moet doen om zijn accountantscontrole te verrichten. KAS ontbeert echter een systematische uiteenzetting van de wijze *waarop* de auditor zijn bedrijfsgerichte controle moet uitvoeren. Er is behoefte aan een stramien waarmee de auditor het bedrijf en zijn omgeving kan analyseren en documenteren.

Met de ontwikkeling van dit stramien is KPMG in het begin van de jaren negentig in de Verenigde Staten onder de naam *Business Measurement Process* gestart. In 1997 werd met de wereldwijde introductie van dit stramien – buiten de Verenigde Staten aangeduid als Audit 2000 – begonnen.

In de praktijk voegt de op risicoanalyse gebaseerde controleaanpak weinig waarde voor de cliënt zelf toe.

Onder KAS is de afgelopen jaren veel voortgang geboekt met de integratie van IRM in de accountantscontrole. Algemeen wordt thans ingezien dat bemoeienis van IRM op zijn plaats is indien de bedrijfsprocessen van de cliënt in meerdere of mindere mate zijn geautomatiseerd. Omtrent de aard van de IRM-activiteiten ten behoeve van de accountantscontrole bevat KAS duidelijke en concrete richtlijnen. Voorts is daaraan in detail invulling gegeven in het Handboek ITAC ([KEA97]). Binnen het bestek van dit artikel is ingegaan op de vraag of de aanvulling van KAS met de Audit 2000-methodologie consequenties heeft voor de wijze waarop IRM de jaarrekeningcontrole kan ondersteunen.

Achtereenvolgens is aandacht besteed aan:
* de achtergrond en de inhoud van Audit 2000;
* een vergelijking tussen Audit 2000 en KAS;
* de betekenis van IRM-activiteiten binnen de Audit 2000-methodologie.

Ontstaan en inhoud van Audit 2000

Generaliserend gesproken ligt de kern van een op risicoanalyse gebaseerde controleaanpak in de identificatie en analyse van risico's op een materiële onjuistheid in de jaarrekening. Daartoe worden posten in de jaarrekening beoordeeld op de aanwezigheid van controle-informatie waarmee volledigheid, bestaan, juistheid, waardering, eigendom en presentatie van die posten kunnen worden vastgesteld. De controleaanpak is daarmee vooral jaarrekeninggericht.

In de praktijk blijkt dat deze benadering weinig waarde voor de cliënt zelf toevoegt. De aanpak doet precies wat binnen de scope van de accountantscontrole past. Namelijk het leggen van een rechtstreeks verband tussen beweringen van het management omtrent posten in de jaarrekening en controlebewijs voor die beweringen. Het controlebewijs betreft dan de aanwezigheid van beheersingsmaatregelen in de processen die de risico's op een materiële fout in de jaarrekening afdekken, alsmede cijferanalyses en aanvullende detailcontroles voor relevante restrisico's in die processen. Het resultaat is een verklaring bij de jaarrekening en een management letter. Omdat binnen de scope van de accountantscontrole de aandacht zich vooral richt op beheersingsmaatregelen die de volledigheid, juistheid en tijdigheid van de aan de posten ten grondslag liggende gegevensverwerkende processen waarborgen, bevat de management letter vooral aandachtspunten en adviezen ter verbetering van deze beheersingsmaatregelen.

Hoewel de rol van de auditor op dit punt niet onbelangrijk is, heeft deze controlebenadering bijgedragen aan het beeld van de auditor als specialist op het gebied van de administratieve organisatie en interne controle en niet als de bedrijfsadviseur zoals de auditor zichzelf graag ziet ([Limp87]). Daarvoor is het vooral nodig dat hij voldoende op de hoogte is met de doelstellingen, strategie en processen van het bedrijf om als een echte gesprekspartner voor zijn cliënt te kunnen dienen.

Een tweede aspect dat heeft bijgedragen aan de ontwikkeling van de Audit 2000-methode is het feit dat het kennen van het bedrijf van de cliënt, zijn doelstellingen, de risico's die de realisatie van die doelstellingen kunnen verhinderen en de wijze waarop de cliënt deze risico's beheerst, de auditor beter in staat stelt audit risks te identificeren. Zoals eerder gesteld ligt deze filosofie al besloten in de KAS-aanpak, maar heeft het tot voor kort ontbroken aan handvatten waarmee de auditor daadwerkelijk de doelstellingen en strategie van zijn cliënt kan analyseren.

Audit 2000 reikt die handvatten aan. Aan de Audit 2000 Methodology Guide ([KPMG97]) ontlenen wij de volgende omschrijving van Audit 2000: 'Audit 2000 is about KPMG professionals around the world using knowledge to transform the audit and the way they work together to deliver client service'.

Elementen van Audit 2000

Aan de basis van de Audit 2000-methode ligt de visie ten grondslag dat bedrijfs- en procesrisico's die in het heden onvoldoende beheerst zijn, vroeg of laat tot jaarrekeningrisico's zullen leiden. Hoe eerder het management zich van deze risico's bewust is, hoe kleiner de kans dat deze risico's op termijn manifest worden en tot bedrijfsverliezen leiden die hun weerslag op de jaarrekening hebben. Hoe nadrukkelijker de analyse door de auditor van bedrijfsrisico's in het heden, hoe kleiner de kans op een toekomstige materiële fout in de jaarrekening die door de auditor te laat wordt ontdekt. De Audit 2000-methodologie bestaat uit de volgende bouwstenen.

Strategiefase (Strategic analysis)
Het doel van de Strategiefase is inzicht te verkrijgen in de bedrijfsdoelstellingen en de strategie van de cliënt. Daarmee kunnen belangrijke bedrijfsrisico's worden geïdentificeerd die mogelijk consequenties hebben voor de controle.

Bedrijfsprocesanalyse (Business process analysis)
Het doel van de Bedrijfsprocesanalyse is het verkrijgen van inzicht in de *key business processes* om daarmee procesrisico's te kunnen identificeren en te bepalen wat de invloed van die risico's op de jaarrekening kan zijn.

Risicobeoordeling (Risk assessment)
Het doel van de Risicobeoordeling is inzicht te krijgen in het proces van risicoanalyse van de cliënt. Nagegaan wordt of de cliënt zijn risico's voldoende beheerst. Daartoe wordt onder andere een analyse uitgevoerd van de strategische en procesrisico's en vooral ook van de wijze waarop het management deze risico's beheerst en de maatregelen die het management heeft getroffen als antwoord op deze risico's.

Bedrijfsmeting (Business measurement)
Tijdens de Strategiefase, de Bedrijfsprocesanalyse en de Risicobeoordeling bouwt de auditor een verwachting op over de prestaties van de cliënt. In de fase van de Bedrijfsmeting valideert de auditor deze verwachtingen aan de hand van de uitkomsten van de bedrijfsprocessen van de cliënt.

Voortdurende verbetering (Continuous improvement)
In de fase van Voortdurende verbetering kan de auditor zijn rol als bedrijfsadviseur ten volle vervullen. Zijn bevindingen in de voorgaande fasen van de Audit 2000-methodologie gebruikt hij om zijn cliënt te adviseren over mogelijke verbeteringen in de bedrijfsvoering.

Vergelijking met KAS

Audit 2000 bouwt voort op de visie en methodologie die in KAS ligt besloten. De richtlijnen en voorschriften in KAS blijven dan ook onverkort van toepassing onder Audit 2000. Zoals gezegd brengt Audit 2000 echter een verdieping aan in de bedrijfs- en proceskennis. Tabel 1 geeft inzicht in de verschillen tussen een op KAS en een op Audit 2000 gebaseerde controlebenadering.

Tabel 1. Verschillen tussen KAS en Audit 2000.

KAS	Audit 2000
Transactiegeoriënteerd Gebaseerd op het idee dat inzicht in het totaal kan worden verkregen door onderzoek van de afzonderlijke delen.	**Holistische benadering** Gebaseerd op het idee dat inzicht in het totaal bijdraagt aan kennis over de afzonderlijke delen.
Nadruk ligt op het proces van informatieverwerking Verwachtingen over de uitkomsten van de bedrijfsprocessen worden opgebouwd door verband te leggen tussen verantwoordingsinformatie.	**Nadruk ligt op de bedrijfsprocessen** Veronderstelt dat de doelstellingen en de bedrijfsstrategie gerealiseerd worden door bedrijfsprocessen. Verwachtingen over de uitkomsten van de bedrijfsprocessen worden opgebouwd door beoordeling van de strategie en procesindicatoren.
Kennis van controlemethoden en -technieken Is gebaseerd op de gedachte dat een diepgaande kennis van controlemethoden en -technieken en verslaggevingsvoorschriften de auditor in staat stelt overeenkomsten en afwijkingen te onderkennen.	**Bedrijfskennis** Is gebaseerd op de gedachte dat een brede kennis van het bedrijf van de cliënt en zijn omgeving de auditor in staat stelt overeenkomsten en afwijkingen te onderkennen.
Losstaande systemen Ziet de organisatie als een set van losstaande systemen die afzonderlijke transacties genereren die onafhankelijk van elkaar kunnen worden beoordeeld.	**Verbonden systemen** Ziet de organisatie als een dynamisch geheel van verbonden systemen die niet onafhankelijk van elkaar kunnen worden beoordeeld.
Auditrisico Gaat ervan uit dat de accountantsverklaring losstaat van de beoordelingen en inschattingen van het bedrijfsrisico door het management.	**Bedrijfsrisico** Gaat ervan uit dat de accountantsverklaring onlosmakelijk is verbonden met de beoordeling en inschatting van bedrijfsrisico's.

Rol van IRM in Audit 2000

De informatie- en communicatietechnologie (ICT) is de afgelopen decennia uitgegroeid tot één van de belangrijkste pijlers voor het functioneren van bedrijven en instellingen. De afhankelijkheid van ICT is thans zo groot dat beschikbaarheid en beveiliging van deze processen van essentieel belang zijn. De investeringen in ICT zijn van majeure omvang. Daarmee is ook de efficiëntie en effectiviteit van automatisering een onderwerp geworden dat meer en meer de agenda van het management beheerst. Het zal duidelijk zijn dat de ICT een kritische succesfactor is geworden bij de realisatie van de bedrijfsdoelstellingen. De ICT van een bedrijf of instelling is dan ook één van de resources die zowel in het strategisch als in het operationele plan is terug te vinden.

Als voorbeeld moge dienen de uitgever die, om een voorsprong op de concurrent te nemen, in zijn strategisch plan aangeeft Internet te willen gebruiken om zijn producten te verkopen (*electronic commerce*). Deze doelstelling kan alleen dan worden bereikt indien de strategie van het ICT-proces aansluit op deze doelstelling. Men zou kunnen zeggen dat het strategisch en operationeel electronic-commerceplan van de uitgever niet volkomen is indien daarin geen aandacht is besteed aan de relatie tussen deze doelstelling en de opzet en uitvoering van het ICT-beleid.

Zoals hiervoor gesteld ligt de kern van de Audit 2000-methode in het identificeren van zogenaamde *key business processes*. Dit zijn de processen met de kenmerken:
* een groot strategisch belang;
* een hoog inherent risico;
* een hoog internecontrolerisico.

Een key business process behoeft niet altijd een primair proces (*core business process*) te zijn. Ook het strategisch managementproces (*strategic management process*) en de ondersteunende processen (*resource management process*) kunnen – indien zij voldoen aan de hierboven gegeven kenmerken – als een key business process worden aangemerkt.

Aan de Audit 2000-methode ligt de visie ten grondslag dat bedrijfs- en procesrisico's die onvoldoende beheerst zijn tot jaarrekeningrisico's zullen leiden.

Traditioneel wordt het ICT-proces als een ondersteunend proces aangemerkt. Het zijn de hulpmiddelen waarmee de producten van het bedrijf of de instelling worden verkocht. Een snelle projectie van de hierboven weergegeven criteria op de ICT van bedrijven en instellingen leidt tot de constatering dat de ICT in veel gevallen hoog scoort op strategie, inherent risico en internecontrolerisico. Deze wetenschap leidt ertoe dat bij de samenstelling van het Audit 2000 *client service team* plaats ingeruimd moet worden voor een IRM-specialist. Hij zal het team namelijk informatie moeten aanleveren waarmee:
* de opdrachtverantwoordelijke beargumenteerd kan besluiten de ICT al dan niet als key business process aan te merken;
* de opdrachtverantwoordelijke duidelijk kan worden gemaakt welke beheersingsmaatregelen aanwezig zijn in applicaties en in de automatiseringsorganisatie ingeval sprake is van substantiële ICT-ondersteuning van een key business process;
* de opdrachtverantwoordelijke duidelijk kan worden gemaakt of het ICT-proces als key business process voldoende wordt beheerst.

Hierna wordt dieper ingegaan op de werkzaamheden die de IRM-specialist in elk van de hiervoor vermelde fasen van Audit 2000 kan uitvoeren zodat de opdrachtverantwoordelijke een antwoord kan geven op deze aspecten.

Algemene betrokkenheid IRM-specialist

Betrokkenheid van een IRM-specialist in het client service team is natuurlijk geen conditio sine qua non. Die betrokkenheid is vooral het resultaat van de uitkomsten van een initiële beoordeling van de omvang en het belang van de ICT bij de cliënt. In het merendeel van de gevallen is sprake van een bestaande relatie en is op basis van ervaringen in het verleden – los van Audit 2000 – reeds een teamsamenstelling gekozen waarin al dan niet een plaats is ingeruimd voor de IRM-specialist.

Voor het vervolg van dit artikel wordt van de veronderstelling uitgegaan dat sprake is van een nieuwe cliënt en er dus geen operationele kennis over de stand van de ICT bij de cliënt aanwezig is. Voorafgaand aan de keuze voor de samenstelling van het team dient het client service team een initiële beoordeling uit te voeren op het ICT-proces van de cliënt. Het doel van het initiële onderzoek is een antwoord te krijgen op de vraag in welke mate de cliënt afhankelijk is van ICT (zie tabel 2). Hiermee kan voorts de basis worden gelegd voor automatiseringsgerichte onderzoeken.

Als de uitkomst van het initieel onderzoek luidt dat de ICT een wezenlijk bestanddeel vormt van de bedrijfsvoering, zodanig dat de uitkomsten van de processen afhankelijk zijn van de kwaliteit van het ICT-proces, dan dient een ICT-specialist aan het client service team te worden toegevoegd.

Omtrent de feitelijke inzet dienen concrete afspraken tussen de opdrachtverantwoordelijke en de IRM-specialist te worden gemaakt. De ervaring leert dat zonder dergelijke afspraken de effectiviteit van een Audit 2000-proces belangrijk afneemt. Opdrachtverantwoordelijke en IRM-specialist hebben dan geen duidelijk beeld van ieders taken en verantwoordelijkheden. De operationele inzet heeft in dat geval geen structuur en de uiteindelijke betrokkenheid en resultaten van werkzaamheden kunnen niet worden geïntegreerd met de resultaten van de werkzaamheden van de andere client-service-teamleden.

De vernieuwing van de controleaanpak door het toepassen van de Audit 2000-methode kan niet van het ene op het andere jaar worden gerealiseerd. Voor het vervolg

Inzicht in de omvang van het ICT-proces	Afhankelijkheid van automatisering	Beheersing van automatisering
* Van welke geautomatiseerde informatiesystemen wordt gebruikgemaakt? * Hoe zijn de geautomatiseerde systemen totstandgekomen? Is er sprake van pakketten of zelfbouw? * Op welk platform vindt de verwerking plaats (mainframe, client/server, WAN, LAN, externe verwerking)? Locaties? * Is er sprake van gebruik van EDI of andere vormen van geavanceerde informatietechnologie? * Is er een aparte automatiseringsorganisatie? * Wat is de omvang van de automatiseringsorganisatie?	* Zijn logistieke processen in belangrijke mate geautomatiseerd? * Zijn belangrijke beslissingen afhankelijk van met behulp van automatisering gegenereerde informatie? * Wat zijn de effecten van uitval van IT-systemen? * Hoe groot is de afhankelijkheid en het gebruik van EDI? * Zijn er problemen met IT-systemen die de bedrijfsuitoefening in belangrijke mate beïnvloeden? Denk hierbij aan: – systemen die niet meer zijn opgewassen tegen de taak; – vertragingen in de verwerking van de gegevens; – oorzaken van storingen. * Zijn er IT-systemen in ontwikkeling of gepland die de bedrijfsuitoefening in belangrijke mate zullen gaan beïnvloeden? Denk hierbij aan: – nieuwe informatiesystemen (standaardpakketten of maatwerkprogrammatuur) die onder meer tot veranderingen in de AO zullen leiden; – aanpassingen in de automatiseringsorganisatie, zoals organisatieveranderingen, verhuizing, uitbesteding, downsizing, etc.; – aanpassingen in de gebruikte computerfaciliteiten; vaak betekent dit ook betere controlemogelijkheden; – informatiesystemen ouder dan vijf jaar; – tijd die wordt besteed aan onderhoud van de informatiesystemen.	* Is er een duidelijk beleid van de organisatie met betrekking tot de automatisering? * Is er de indruk dat door de organisatie gesteund wordt op computercontroles ter waarborging van de betrouwbaarheid en continuïteit van de informatievoorziening? * Is er bij het management aandacht voor beveiliging (toegangscontrole, etc.)? * Ontvangt het management regelmatig informatie met betrekking tot de stand van zaken bij de automatisering (periodiek overleg, via stuurgroep, budget)?

Tabel 2.
Initieel onderzoek stand automatisering.

van dit artikel wordt echter uitgegaan van het hypothetische geval dat bij de hiervoor geïntroduceerde nieuwe cliënt de volledige Audit 2000-methodologie in het eerste jaar direct in volle omvang wordt toegepast.

Strategiefase

In de Strategiefase zijn de taken van de IRM-specialist erop gericht na te gaan of de ICT-processen de doelstellingen en strategie van de cliënt voldoende ondersteunen. Zoals hiervoor is gesteld, is het niet aansluiten van dit proces op de bedrijfsstrategie een belangrijk bedrijfsrisico dat ongetwijfeld in een auditrisico zal culmineren indien het management van de cliënt geen gepaste maatregelen daartegen neemt. Daarmee vervult de IRM-specialist een belangrijke rol in het client service team bij het inkaderen van het totaal aan bedrijfsrisico's en de beheersing daarvan door de cliënt.

Aandacht voor de ICT-strategie in het algemeen betekent bovenal dat de IRM-specialist voldoende op de hoogte is van ontwikkelingen en trends op ICT-gebied. Voorwaar geen sinecure gelet op de snelheid en omvang waarmee ICT-ontwikkelingen en -vernieuwingen op ons afkomen. Vakbladen en elektronische informatiebronnen kunnen een goede dienst bewijzen. Natuurlijk zal de IRM-specialist zijn vakliteratuur zorgvuldig bijhouden. Tegelijk is het een illusie te veronderstellen dat één persoon alle ICT-ontwikkelingen op de voet zou kunnen volgen. Binnen de IRM-discipline – zoals bij KPMG EDP Auditors (KEA) – heeft dit tot een specialisatie geleid waarbij zogenaamde productontwikkelgroepen verantwoordelijk zijn voor de ontwikkeling en het onderhoud van de dienstverlening en het verspreiden van kennis binnen de werkmaatschappij. Langs deze weg is het voor elke IRM-specialist mogelijk zich op de hoogte te stellen van de productontwikkeling binnen KEA, waarmee hij de ICT-ontwikkelingen van de cliënt binnen een perspectief kan plaatsen. Dat gevoegd bij de kennis die tot hem komt via vakbladen en andere media stelt hem beter in staat risico's in de ICT-ontwikkeling bij de cliënt te identificeren.

Naast inbreng van algemene kennis kan de IRM-specialist in de Strategiefase specifiek ICT-gericht onderzoek vervullen. Doelstelling daarvan is dat hij in staat is voor het client service team zichtbaar te maken of de strategische IT-risico's voldoende worden beheerst. Thans bestaan binnen KEA twee producten waarmee dit onderzoek kan worden verricht. Het eerste is een meer globale en algemene beoordeling van de kwaliteit van de IT-organisatie, de '*IT Controls Benchmark*', in het bijzonder gericht op de mate waarin de ICT-organisatie de betrouwbaarheid en continuïteit van de ICT kan waarborgen. Het andere product is meer specifiek gericht op het in kaart brengen van de strategische ICT-doelstellingen, beoordeling daarvan en formulering van adviezen en aanbevelingen. Dit product wordt aangeduid met '*Strategic Alignment*' en maakt onderdeel uit van een breder geheel van ICT-dienstverlening onder de naam

World Class IT. Op de inhoud van beide producten is hierna dieper ingegaan.

IT Controls Benchmark (ITCBM)

De ITCBM is een product dat binnen de IRM-praktijk wordt toegepast om inzicht te bieden in de mate waarin IT wordt beheerst door de cliënt. In het bijzonder zijn hierbij aspecten gekozen die relevant zijn in het kader van het waarborgen van de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking. De ITCBM is in internationaal samenwerkingsverband tussen IRM-zusterfirma's ontwikkeld.

Aan de cliënt wordt een standaardvragenlijst verschaft met het verzoek deze vragen te laten beantwoorden door gebruikers en medewerkers van de automatiseringsorganisatie. De standaardvragenlijst richt zich op de identificatie van beheersingsmaatregelen die het risico van inbreuken op de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking moeten tegengaan. De aspecten die in de ITCBM aan de orde komen zijn:

* beleid en management;
* systeemontwikkeling;
* exploitatie & beheer;
* continuïteit;
* beveiliging van informatie en systemen.

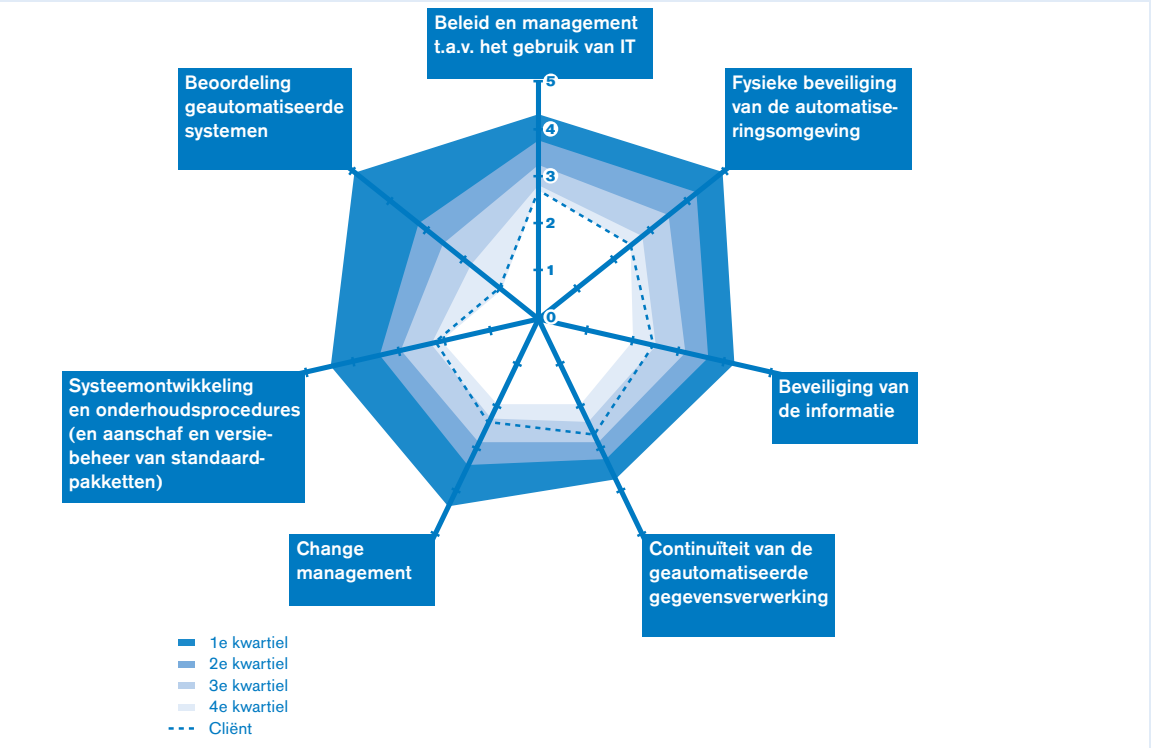
De antwoorden worden vervolgens door een IRM-specialist doorgenomen met de invuller. Daarbij wordt ook zoveel mogelijk vastgesteld dat de door de invuller vermelde beheersingsmaatregelen bestaan. De antwoorden worden in een database ingevoerd en de resultaten van de inventarisatie en beoordeling van de beheersingsmaatregelen worden afgezet tegen die van soortgelijke bedrijven of instellingen. Dit proces is thans beter bekend onder het begrip benchmarking.

De benchmarkresultaten worden vervolgens in de vorm van een presentatie teruggekoppeld aan de cliënt. De presentatie heeft een zodanige vorm (zie figuur 1) dat zij de cliënt in staat stelt het per IT-aspect gemeten niveau te relateren aan de verschillende kwaliteitsniveaus zoals die in de database zijn opgenomen. Afhankelijk van het ambitieniveau van de cliënt kan hij daarmee zijn doelstellingen voor de gewenste kwaliteit per IT-aspect bijstellen en dit vervolgens als norm voor de beheersing van IT opleggen.

De ITCBM is hiermee een product dat uitermate goed past in de Audit 2000-methodiek. Ten eerste wordt het ICT-proces centraal gesteld en identificeert het risico's die onvoldoende in het proces worden beheerst. Daarmee geeft het invulling aan de *Bedrijfsprocesanalyse* en *Risicobeoordeling* van Audit 2000. Vervolgens wordt het kwaliteitsniveau van de IT-aspecten gemeten en afgezet tegen het kwaliteitsniveau van branchegenoten. Dit proces maakt onderdeel uit van *Bedrijfsmeting*. De uitkomsten stellen het client service team in staat gericht te adviseren over aan te brengen verbeteringen in het ICT-proces (*Voortdurende verbetering*). Tevens sluit de manier van werken (benchmarken) veelal direct aan op de behoeften van het management.

World Class IT

WCIT is een internationaal KPMG-platform. Deskundigen uit verschillende KPMG-landen hebben hun ICT-kennis en -ervaring samengebracht en uitgewerkt in een geïntegreerde set methoden en technieken. Daarmee kan de performance van ICT binnen organisaties worden



Figuur 1. Benchmarkpresentatie IT Controls Benchmark.

beoordeeld en kunnen organisaties gericht worden geadviseerd over maatregelen die getroffen kunnen worden om de performance te verbeteren.

De aandachtsgebieden van WCIT kunnen als volgt schematisch worden weergegeven.

Het onderdeel 'Strategic Alignment' richt zich in het bijzonder op informatiebeleid en planning; het aan elkaar relateren van bedrijfsbeleid, IT-beleid, informatiebeleid en informatieplanning. In overleg met de opdrachtverantwoordelijke van het client service team en de cliënt kan de diepgang van de beoordeling nader worden ingevuld.

Bedrijfsprocesanalyse

Uiteindelijk gaat het er in deze fase van de Audit 2000-methode om dat key business processes worden geanalyseerd op de mate waarin procesrisico's daarin worden beheerst. Als wij kijken naar het ICT-proces binnen een bedrijf dan kan dit op tweeërlei wijze in de Bedrijfsprocesanalyse tot uitdrukking komen:

* Het ICT-proces zelf moet als een key business process worden aangemerkt.
* ICT-objecten spelen een belangrijke ondersteunende rol in een key business process niet zijnde het ICT-proces zelf.

Als voorbeeld moge het volgende dienen. Veronderstel dat het ICT-proces een essentiële maar vooral kritieke factor in de gehele bedrijfsvoering van de cliënt vormt. Uitval leidt tot continuïteitsrisico's en de ICT is een kritieke succesfactor bij het realiseren van de doelstellingen van de cliënt. Tot slot bestaat de indruk na een globale beoordeling van de automatiseringscontroleomgeving dat het ICT-proces niet volledig 'in control' is. Hier is zonder twijfel sprake van ICT als key business process.

Van ICT-objecten die ondersteunend zijn aan een key business process kan bijvoorbeeld sprake zijn bij een chemisch bedrijf waarin zowel productieplanning als verkoopplanning een centrale rol vervult in de bedrijfsvoering en beide processen voor de realisatie van de procesdoelstellingen in belangrijke mate afhankelijk zijn van een informatiesysteem dat een groot gedeelte van beide processen ondersteunt. In dat geval is ICT niet een key business process, maar zal de ICT wel object van beoordeling zijn bij de verdere analyse van dit proces (zie hierna).

Of het ICT-proces als key business process moet worden aangemerkt, wordt onder meer bepaald door de in tabel 3 opgenomen vragen die de IRM-specialist zal moeten onderzoeken.

Als het ICT-proces als key business process wordt aangemerkt, ziet het client service team zich voor de keuze geplaatst welke componenten van het ICT-proces aan een nadere analyse te onderwerpen. Het ICT-proces kan daarbij op verschillende wijzen worden afgebeeld[2]. Als de insteek van het WCIT-hulpmiddel wordt gekozen, dient het client service team de keuze te bepalen op één of meer van de componenten die in figuur 2 zijn vermeld. De keuze wordt bepaald op basis van een verdere verdieping van de vraag welke componenten het meest hebben bijgedragen in de beslissing het ICT-proces als een key business process aan te merken. De diepgang waarmee het onderzoek wordt uitgevoerd, is een zaak van professionele oordeelsvorming en is mede afhankelijk van de aard van het bedrijfsproces, de omvang van het ICT-proces, omgevingsfactoren, eventuele wensen van de cliënt, etc. De stappen die vervolgens worden uitgevoerd, zijn:

* *intake-gesprek*. Het betreft hier de afbakening van het onderzoek met de organisatie. Bepaald wordt welke aspecten van de gekozen ICT-componenten ter hand zullen worden genomen.
* *pre-auditvragenlijst*. Om het onderzoek zo efficiënt mogelijk te laten verlopen wordt vooraf zoveel mogelijk geïnventariseerd welke documentatie aanwezig is en welke medewerkers moeten worden geïnterviewd. Aan de hand van een pre-auditvragenlijst worden met de cliënt afspraken gemaakt over beschikbaarheid, tijdstippen en doorlooptijd.
* *bestudering documentatie*. Documentatie over de te onderzoeken IT-componenten wordt door de IRM-specialist bestudeerd. De binnen WCIT ontwikkelde criteria worden toegepast, leidend tot eerste bevindingen en conclusies.
* *interviews*. Belangrijke spelers binnen de te onderzoeken IT-componenten worden geïnterviewd. Voorlopige bevindingen en conclusies worden afgestemd.
* *analyseren van onderzoeksresultaten*. De uitkomsten van het bestuderen van documentatie en afnemen van interviews worden geanalyseerd en op gestructureerde wijze in kaart gebracht. De uitkomsten worden gerelateerd aan soortgelijke organisaties. Daarmee kan de cliënt zijn situatie relateren aan die van andere organisaties. Op basis daarvan kunnen aanbevelingen worden gedaan.
* *bespreking resultaten*. In de vorm van een presentatie worden de resultaten besproken met de cliënt.

Langs deze weg is het mogelijk IT als ondersteunend proces te beoordelen. Aan het eind van de opdracht bestaat een goed beeld over de beheersing van de onderzochte IT-componenten. Opgemerkt wordt dat KEA voor het onderzoek naar de kwaliteit van elk van de WCIT-componenten ook een Quick Scan-variant heeft ontwikkeld. Daarmee kan in korter tijdsbestek maar ook met een geringere diepgang inzicht worden verkregen in eventuele knelpunten in de onderzochte IT-component.

2) Als insteek kan bijvoorbeeld de indeling in de managementdisciplines van de ITIL-beheerprocessen worden gekozen.

Figuur 2. Aandachtsgebieden World Class IT.

Wat is het strategisch belang van het ICT-proces bij de realisatie van de bedrijfsdoelstellingen?
* Zijn de primaire processen geautomatiseerd?
* Wat is de betekenis van de automatisering voor de uitvoering van die primaire processen?
* Wat zijn de consequenties van uitval van deze automatisering voor de operationele uitvoering van de primaire processen?
* In hoeverre worden de bevindingen en conclusies van de IRM-specialist bevestigd door de uitkomsten van een namens de leiding uitgevoerde gevoeligheidsanalyse?
* In hoeverre is de meet- en stuurinformatie over de uitkomsten van het primaire proces afkomstig van geautomatiseerde systemen?
* Wat is de consequentie van uitval van deze systemen voor de beheersing van het primaire proces?
* Wat is de visie van het management op het belang en de gevoeligheid van de systemen die meet- en stuurinformatie leveren?

Wat is het inherente risico dat verbonden is aan het ICT-proces? Factoren die daarbij een rol spelen zijn onder andere:
* impact van strategische risico's op het ICT-proces;
* de complexiteit van het ICT-proces;
* de mate waarin oordeelsvorming door het management in het ICT-proces een rol speelt;
* sterkte van de beheersomgeving;
* de ervaring die het client service team heeft met de beheersing van het ICT-proces;
* de mate waarin bepaalde gebeurtenissen gevolgen kunnen hebben voor de werking van het ICT-proces.

In hoeverre wordt het ICT-proces beheerst? Op dit niveau wordt voor de beantwoording van deze vraag in belangrijke mate gebruikgemaakt van de informatie die tijdens de *Strategiefase* is vergaard. In die fase is reeds inzicht verkregen in de beheersomgeving. Zoals hiervoor is aangegeven, is in deze fase ten aanzien van de ICT bijvoorbeeld door middel van toepassing van de ITCBM informatie verkregen over de beheersomgeving. Vragen waarop een antwoord gegeven kan worden, betreffen:
* Heeft de cliënt een formeel en informeel beleid voor het niveau en de wijze waarop het ICT-proces wordt beheerst?
* Houdt de cliënt toezicht op de resultaten van het ICT-proces?
* Reageert de leiding tijdig op veranderingen in de externe omgeving die van invloed kunnen zijn op de uitgangspunten en het operationele beheer van het ICT-proces?
* Zijn de geautomatiseerde systemen stabiel en is er bewijs voor de effectieve werking van deze systemen over de afgelopen jaren?
* Wordt snel en adequaat gereageerd door de leiding op verstoringen in het ICT-proces?

Tabel 3. Onderzoek ICT als key business process.

Indien wordt geconcludeerd dat niet het ICT-proces zelf als key business process moet worden aangemerkt, maar ICT-objecten wel een belangrijke ondersteunende rol vervullen in key business processes, zal de IRM-specialist gebruikmaken van het in internationaal verband ontwikkelde KPMG-tool *Business Process Analysis (BPA)*.

Het object van onderzoek van BPA is het bedrijfsproces (of een deel van dit proces) inclusief de informatiesystemen (of deel van de systemen) die het proces ondersteunen. Dus de applicatie(s) (programmatuur en bestanden) én de daarbij behorende handmatige handelingen. Het doel van BPA is het beoordelen van processen op de aanwezigheid van *procescontrols* die de procesrisico's afdekken. De procescontrols kunnen een combinatie zijn van geprogrammeerde controles en gebruikerscontroles (tezamen wel aangeduid als toepassingscontroles).

BPA kent de volgende fasering:
* Strategic analysis;
* Documentation;
* Risk assessment;
* Identify controls;
* Assess residual risk;
* Test controls.

Wat onmiddellijk opvalt is de aansluiting tussen de BPA-fasering en de fasering van de Audit 2000-methode. Het zal dan ook niet verbazen dat de fase *Strategic analysis* vooral gericht is op het verkrijgen van inzicht in het bedrijf, de strategie, de bedrijfsrisico's en -doelstellingen, de bedrijfsprocessen en de IT-omgeving. Vanzelfsprekend zal daarbij zoveel mogelijk gebruik worden gemaakt van informatie die reeds beschikbaar is bij het client service team en bijvoorbeeld tijdens de Strategiefase van de Audit 2000-methode is verzameld.

De resultaten van elk van de zes fasen van BPA worden op een gestructureerde wijze vastgelegd in tabellen. De precieze vorm van de tabellen kan van opdracht tot opdracht verschillen en is dan ook niet binnen de BPA-methode voorgeschreven. Zij zal één of meer van de volgende elementen kunnen bevatten (zie figuur 3).

De fase van *Documentation* heeft tot doel het inzicht in het proces en in het bijzonder de ondersteunende informatiesystemen te verdiepen. Belangrijk is dat bij BPA de processtappen of activiteiten (inclusief mogelijke handmatige handelingen) in kaart worden gebracht. Aan de hand van interviews/workshops, de business models, recordlay-outs (datamodellen), deelbeschrijvingen database (view, subschema), invoerschermen, output, toelichting/documentatie systeemontwerper/programmeur, toelichting/documentatie systeembeheerder/gebruiker en overige systeemdocumentatie worden de volgende stappen in de Documentation-fase uitgevoerd:
1 analyseren gegevensstromen (input/output) proces;
2 identificeren van activiteiten;
3 maken schema met toelichting en invullen matrix;
4 verificatie.

In de fase van *Risk assessment* worden de risico's, risicoinschatting en normen van de BPA-tabel ingevuld. Allereerst worden per onderkende activiteit de bedrijfsrisico's vastgesteld, waarbij uiteraard de opgedane kennis in de fase Strategic analysis wordt meegenomen.Vervolgens

Proces	Input	Output	Bedrijfs-risico	Risico-inschatting	Normen	Beheersmaatregelen	Rest-risico
Activiteiten	...	...	...	...	...	...	...
	...	...	...	...	...	...	...

Figuur 3. BPA-tabel.

wordt een inschatting gemaakt van de grootte van het risico. Deze risico-inschatting is een combinatie van de kans dat een risico zich voordoet en de impact daarvan.

In de fasen *Identify controls* en *Assess residual risk* zal de IRM-specialist voor elke norm vaststellen aan de hand van documentatie, waarnemingen en interviews welke beheersingsmaatregelen daadwerkelijk door het management zijn getroffen. Dit betreffen, zoals eerder reeds gezegd, zowel geprogrammeerde controles als gebruikerscontroles. Uiteraard is verificatie ook bij deze fase een vast onderdeel. Nadat de geïdentificeerde beheersingsmaatregelen zijn vastgelegd in de BPA-tabel zal de IRM-specialist het restrisico bepalen. Hierbij stelt de specialist vast of de getroffen beheersingsmaatregelen toereikend zijn om het procesrisico te beheersen.

In de fase *Test controls* kan de IRM-specialist er op verzoek van het client service team toe overgaan de werking van de geïdentificeerde gebruikerscontroles te testen.

BPA is als tool bij uitstek geschikt om toe te passen in een multidisciplinair client service team. De verschillende fasen lenen zich voor een goede taakverdeling tussen de leden van het team. Het toepassen van de BPA-methode is niet bij uitsluiting voorbehouden aan de IRM-specialist. Het identificeren van de activiteiten binnen het proces, de risico's, risico-inschatting en normen kunnen ook door de andere leden van het client service team met ondersteuning van de IRM-specialist worden uitgevoerd. Het beoordelen en verifiëren van de daadwerkelijk getroffen beheersingsmaatregelen zal als het om geprogrammeerde controles gaat meer inzicht in de applicatie vereisen. Daarom zal het meer voor de hand liggen dat de IRM-specialist dit onderdeel voor zijn rekening neemt. Het uiteindelijke resultaat van de gemeenschappelijke inspanningen is een gedetailleerd inzicht in de kwaliteit van de beheersingsmaatregelen binnen de bedrijfsprocessen.

Risicobeoordeling

Deze fase van de Audit 2000-methode staat niet op zichzelf. De toepassing van de methoden en technieken die inzicht dienen te geven in het proces van risicobeoordeling en -beheersing door de cliënt zijn verweven in de Strategiefase en de Bedrijfsprocesanalyse. Dit geldt ook voor de toepassing van de hiervoor vermelde IRM-hulpmiddelen. De risicobeoordeling en risicobeheersing door de cliënt vormt een integraal onderdeel van deze hulpmiddelen.

Bedrijfsmeting

In deze fase van de Audit 2000-methode gaat het om het valideren van de verwachtingen die het client service team heeft omtrent de uitkomsten van de bedrijfsprocessen van de cliënt. Daarbij wordt zowel gebruikgemaakt van financiële als van niet-financiële informatie. Eventuele afwijkingen tussen verwachtingen van het client service team en de uitkomsten van de beoordeelde processen kunnen duiden op bijzonderheden in de processen die nader moeten worden onderzocht.

De hiervoor besproken IRM-producten dragen bij aan het leveren van niet-financiële informatie over het ICT-proces en/of de informatiesystemen die ondersteunend zijn aan de key business processes. Van het ICT-proces dat ondersteunend is aan key business processes mag verwacht worden dat het betrouwbare en tijdige informatie levert waarmee het management van de cliënt het key business process kan sturen. De uitkomsten van de IRM-hulpmiddelen IT Controls Benchmark, World Class IT en Business Process Analysis moeten duidelijk maken in hoeverre het ICT-proces en/of de informatiesystemen daartoe in staat zijn.

> Business Process Analysis is als tool bij uitstek geschikt om toe te passen in een multidisciplinair client service team.

Indien het ICT-proces zelf als key business process is aangemerkt, zal het vooral het World Class IT-product zijn dat moet duidelijk maken in hoeverre het ICT-proces functioneert conform de doelstellingen van de cliënt. Daarbij kunnen ook andere aspecten dan betrouwbaarheid en tijdigheid van belang zijn (bijvoorbeeld de efficiëntie of effectiviteit van het ICT-proces). De uitkomsten verschaffen informatie over de kwaliteit van het proces. Afwijkingen ten opzichte van de door het management van de cliënt gestelde doelen kunnen duiden op onbeheerste risico's die implicaties kunnen hebben voor de jaarrekening. Navolgend voorbeeld verduidelijkt een en ander.

Veronderstel dat de cliënt een ontwikkelings- en implementatieproject is gestart van een nieuw ERP (Enterprise Resource Planning)-pakket. De investeringen zijn omvangrijk. De cliënt heeft geen ervaring met een dergelijk grootschalig project. Het welslagen van het project is uitermate belangrijk voor de efficiëntie van de bedrijfsvoering en de positie van de cliënt in de bedrijfstak. Dit deel van het ICT-proces (systeemontwikkeling en implementatie) is aangemerkt als key business process. Het World Class IT-product wordt ingezet voor de beoordeling van het ontwikkelings- en implementatieproject. In de initiële fase van het project zijn door het management van de cliënt mijlpalen en normen gedefinieerd voor de (tussen)producten van het project. Bij onderzoek blijkt dat deze normen alsmede de gestelde mijlpalen niet worden gehaald. Dit wordt besproken met het management dat inmiddels ook signalen heeft ontvangen over de slechte (functionele) kwaliteit van de opgeleverde tussenproducten. De IRM-specialist koppelt de bevindingen terug naar het client service team dat zich voor de vraag gesteld ziet of dit bedrijfsrisico consequenties heeft voor de door het management geactiveerde ontwikkelingskosten.

Voortdurende verbetering

De resultaten van het toepassen van de IT Controls Benchmark, de World Class IT en de Business Process Analysis worden voorgelegd aan de cliënt tezamen met adviezen om eventueel geconstateerde afwijkingen tussen

doelstellingen en uitkomsten van de procesvoering op te heffen. Bij de eerste twee hulpmiddelen wordt uitvoerig gebruikgemaakt van grafische toepassingen om de cliënt snel inzicht te bieden in de uitkomsten van de werkzaamheden. Geen uitvoerige beschrijvingen van bevindingen en aanbevelingen, maar korte, duidelijke grafische analyses en puntige aanbevelingen.

De uitkomsten van de Business Process Analysis zijn een mengeling van korte procesanalyses voor processen die op hoog niveau zijn beoordeeld, alsmede gedetailleerde weergaven van activiteiten, risico's, normen en 'controls' van key business processes in de vorm van BPA-tabellen. Deze tabellen maken het zowel de cliënt als het client service team mogelijk tekortkomingen in de 'controls' te identificeren en corrigerende maatregelen te treffen.

Tot besluit

In dit artikel is ingegaan op de plaats en betekenis van IRM-werkzaamheden in het kader van KPMG's vernieuwde controleaanpak Audit 2000. Daarbij is een drietal bestaande IRM-hulpmiddelen toegelicht. Aangegeven is dat de *IT Controls Benchmark*, de *World Class IT* en de *Business Process Analysis* een cruciale rol spelen bij het in kaart brengen van de strategic en process controls van het ICT-proces, zowel in het geval dit proces als key business process moet worden aangemerkt, als in het geval dat ICT-objecten ondersteunend zijn aan key business processes, anders dan het ICT-proces.

Literatuur

[Aals98]
Drs. M.W. van Aalst en drs. ing. P. Olieman, *Strategie en informatietechnologie*, Compact 1998/2.

[Bell97]
T.B Bell, F.O. Marrs, I. Solomon, H. Thomas, *Auditing Organizations Through a Strategic-Systems Lens*, KPMG interne publicatie, 1997.

[KEA97]
KPMG EDP Auditors, *Handboek Informatietechnologie en accountantscontrole*, 1e versie, KPMG EDP Auditors interne publicatie, 1997.

[Koed99]
Mw. drs. M.J.A. Koedijk, *Van systeembeoordeling naar procesbeoordeling*, Compact 1999/2-3.

[KPMG94]
KPMG, *Handboek KPMG Audit Service*, KPMG interne publicatie, 1994.

[KPMG97]
KPMG, *Audit 2000 Methodology Guide*, KPMG interne publicatie, 1997.

[Limp87]
Limperg Instituut, *Opvattingen over accountants*, Limperg Instituut, 1987.