De rol van de accountant in ERP-implementatieprojecten

De System Integration Controls-methode

Drs. ing. A.M. Meuldijk

Dit artikel gaat over de door KPMG Information Risk Management (IRM) internationaal ontwikkelde System Integration Controls (SIC)-methode. Deze SIC-methode kan onder andere door de accountant (in samenwerking met ICT-auditors) worden gebruikt om op gestructureerde en proactieve wijze ICT-beheersmaatregelen te beoordelen tijdens of na implementatie van Enterprise Resource Planning (ERP)-systemen. In dit artikel wordt het ERP-systeem SAP R/3 als voorbeeld gebruikt.

Inleiding

Veel organisaties waarbij accountants een verklaring bij de jaarrekening afgeven besluiten de bedrijfsprocessen te ondersteunen met een Enterprise Resource Planning (ERP)-systeem. De bedrijfsprocessen in de organisatie en de getroffen maatregelen van administratieve organisatie en interne controle (AO/IC), waarop de accountant in toenemende mate het oordeel over de getrouwheid van de jaarrekening baseert, zullen als gevolg van de introductie van een ERP-systeem veranderen. Een ERP-systeem wordt namelijk gekenmerkt door het feit dat het sterk geïntegreerde functionaliteit biedt ter ondersteuning van vrijwel alle organisatieonderdelen. Het ERP-systeem integreert bijvoorbeeld de gegevensverzamelingen van verschillende afdelingen, zoals Inkoop, Productie, Verkoop en Financiën. De accountant zal zich derhalve moeten afvragen welke invloed deze integratie heeft op bijvoorbeeld de werkwijzen van het bedrijf en op de functiescheiding die het tegengestelde belang tussen bedrijfsfuncties moet waarborgen. Voor de accountant is het daarom van belang antwoord te krijgen op de vraag wat de invloed is van de introductie van een ERP-systeem op de bedrijfsprocessen en de AO/IC, en voorts wat hiervan de invloed is op de controleaanpak.

De internationale System Integration Controls (SIC)-methode is ontwikkeld voor het uitvoeren van IRM-audit- en adviesopdrachten in het kader van het beoordelen, ontwerpen en ontwikkelen van ICT-beheersmaatregelen gelijktijdig met de uitvoering van een ERP-implementatietraject. De SIC-methode kan tevens door de accountant (in samenwerking met een ICT-auditor) worden gebruikt om al tijdens het implementatieproject op gestructureerde en proactieve wijze ICT-beheersmaatregelen te beoordelen of zelfs te ondersteunen bij het inrichten van ICT-beheersmaatregelen. In dit artikel wordt de SIC-methode beschreven en wordt aangegeven op welke wijze de accountant deze methode kan inzetten in (bijzondere) audit- en adviesopdrachten.

Eerst wordt ingegaan op de rol van de accountant bij ERP-implementaties. Vervolgens wordt de implementatiemethode ASAP (Accelerated SAP) voor het ERP-systeem SAP R/3 besproken, waardoor enig inzicht wordt verkregen in ERP-implementatieprojecten en de mate waarin deze implementatiemethode aandacht besteedt aan AO/IC. Daarna wordt de SIC-methode besproken. Tot slot wordt aangegeven op welke wijze de SIC-methode kan worden ingezet in de accountantscontrole en wat hierin de rollen van de accountant en de ICT-auditor kunnen zijn.

De accountant en ERP-projecten

Om een idee te krijgen van de wijzigingen in de maatregelen van AO/IC (gebruikerscontroles, geprogrammeerde controles en algemene computercontroles) als gevolg van de implementatie van een ERP-systeem en voorts de invloed van deze wijzigingen op de accountantscontrole, kan de accountant twee methoden van aanpak hanteren. In de eerste en meest gehanteerde aanpak wacht de accountant tot het systeem is geïmplementeerd en bepaalt (eventueel met behulp van een ICT-auditor) door middel van een proces- en risicoanalyse wat de invloed is op de accountantscontrole. Het nadeel van deze aanpak is dat de uit het onderzoek voortgekomen aanbevelingen pas na implementatie worden geformuleerd. Als de aanbevelingen gericht zijn op het treffen van aanvullende beheersmaatregelen in het ERP-systeem (geprogrammeerde controles), staat de organisatie voor een keuze. De organisatie kan ofwel de aanvullende beheersmaatregelen alsnog implementeren (inrichten of programmeren) in het ERP-systeem, ofwel de gewenste geprogrammeerde beheersmaatregel compenseren door een aanvullende beheersmaatregel in de gebruikersorganisatie te implementeren (gebruikerscontrole).

Organisaties zijn geneigd voor de tweede optie te kiezen. Het realiseren van een geprogrammeerde controle vereist namelijk meer inspanning en capaciteit dan het implementeren van een gebruikerscontrole. Daarnaast vinden organisaties het veelal niet wenselijk veel wijzigingen door te voeren op het zojuist geïmplementeerde ERP-systeem.

Een geprogrammeerde controle compenseren door een gebruikerscontrole is echter in veel gevallen een inefficiënte oplossing, omdat routinematige controles dan handmatig moeten worden uitgevoerd. Daarnaast is de mate waarin een gebruikerscontrole de betrouwbaarheid van gegevensverwerking waarborgt afhankelijk van de kwaliteit van de door betrokken functionarissen uitgevoerde werkzaamheden. In sommige gevallen kan een geprogrammeerde controle zelfs niet geheel worden gecompenseerd door een gebruikerscontrole, waardoor

Een geprogrammeerde controle compenseren door een gebruikerscontrole is in veel gevallen een inefficiënte oplossing.

een hiaat in de AO/IC ontstaat. Veel geprogrammeerde controles die worden gecompenseerd met gebruikerscontroles, leiden daardoor tot aanvullende controlewerkzaamheden voor de accountant. Daarnaast druist de verminderde waarborg voor de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking regelrecht in tegen de verwachte voordelen van de introductie van een ERP-systeem: de gegevensverwerking wordt effectiever, efficiënter en betrouwbaarder.

Het voorgaande kan voor de accountant een reden zijn om, vanuit de adviesfunctie, al tijdens het implementatieproject te adviseren over wijzigingen in de AO/IC die het gevolg zijn van de introductie van een ERP-systeem. Dit leidt naar de tweede aanpak die de accountant kan hanteren om een beeld te krijgen van de gevolgen van de introductie van een ERP-systeem: de accountant is, eventueel ondersteund door een ICT-auditor, betrokken bij het implementatieproject en beoordeelt (en adviseert) in verschillende projectfasen over de inrichting van de AO/IC. Het voordeel van deze aanpak is dat de aanbevelingen van de accountant tijdens het implementatieproject worden geformuleerd en daardoor nog tijdens de uitvoering van het implementatieproject kunnen worden meegenomen. Daarnaast heeft de accountant aan het einde van de implementatie een goed beeld van de wijziging in de AO/IC en de controleaanpak.

Om invulling te kunnen geven aan de hierboven beschreven aanpak moet de accountant in de eerste plaats weten in hoeverre gesteund kan worden op implementatiemethoden voor een ERP-systeem. Daarom wordt hierna eerst de standaard-implementatiemethode ASAP beschreven. Vervolgens wordt verder ingegaan op de SIC-methode en de wijze waarop accountants deze methode kunnen gebruiken.

ERP-implementatieprojecten

De meeste organisaties hanteren bij de implementatie van een ERP-systeem een standaard-projectaanpak. Een voorbeeld hiervan is de ASAP-methode voor de implementatie van het ERP-systeem SAP R/3. Hierna wordt de ASAP-methode in meer detail beschreven. Eerst worden de verschillende fasen van ASAP toegelicht. Vervolgens wordt kort ingegaan op de hulpmiddelen ('accelerators') die ASAP biedt om te komen tot een gestructureerde en kwalitatief hoogwaardige projectuitvoering. Tot slot wordt besproken in welke mate er binnen ASAP aandacht is voor AO/IC.

ASAP-fasen

Standaard ERP-implementatiemethoden bestaan meestal uit een aantal fasen. Deze fasering houdt in:
* voorbereiden en starten van het implementatieproject;
* ontwerpen van functionele en technische specificaties;
* inrichten van het ERP-systeem en programmeren van aanvullend maatwerk;
* test, acceptatie en voorbereidingen voor overgang naar productie;
* migratie naar productie, nazorg en afsluiting.

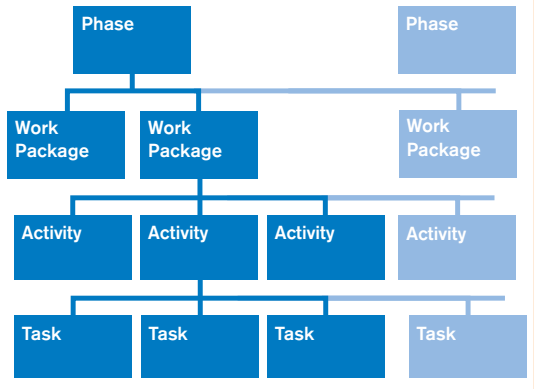
Ook de ASAP-methode kent een dergelijke fasering. De ASAP-methode onderscheidt in de zogenoemde ASAP Roadmap (zie figuur 1) vijf fasen die overeenkomen met de hierboven beschreven fasering. De fasering van ASAP betreft:
1. Project Preparation;
2. Business Blueprint;
3. Realisation;
4. Final Preparation;
5. Go Live & Support.

Figuur 1. ASAP Roadmap ([SAP99]).

In ASAP worden (overeenkomstig andere ERP-implementatiemethoden) de werkzaamheden die door het projectteam ten behoeve van de hierboven genoemde projectfasen moeten worden uitgevoerd, opgedeeld in een hiërarchie van taakclusters (een Work Breakdown Structure (WBS), figuur 2). Hierbij wordt in ASAP onderscheid gemaakt in Phases (projectfasen), Work Packages, Activities en Tasks. Een reeks van samenhangende Tasks vormt een Activity, een reeks van samenhangende Activities vormt een Work Package en een aantal samenhangende Work Packages vormt een Phase. Tot op Task-niveau is in ASAP in detail beschreven welk deelproduct wordt opgeleverd, wat de ingangseisen zijn, welke hulpmiddelen ondersteunen, etc. ([Koed99a]).

Hieronder worden de projectfasen van ASAP in het kort besproken.

Project Preparation Phase
De eerste fase van de ASAP-methode is de voorbereidingsfase. Het doel van deze fase is te komen tot een planning en de voorbereiding van het project. Deze fase ondersteunt in het vaststellen van de primaire focus van het project, terwijl ruimte blijft voor specifieke doelen, verdere afbakening en prioriteiten. De ASAP-methode



Figuur 2. Work Breakdown Structure.

beoogt met deze fase een solide basis te leggen voor een succesvolle implementatie.

In de Project Preparation Phase staat een aantal aspecten centraal. Dit zijn:
* het vaststellen van projectdoelstellingen;
* het vaststellen van de implementatiescope;
* het definiëren van de implementatiestrategie;
* het definiëren van de overallplanning en implementatievolgorde;
* het opzetten van de projectorganisatie en werkgroepen;
* het aanstellen van projectmedewerkers.

Business Blueprint Phase
Het doel van de Business Blueprint Phase is het opstellen van de functionele eisen die aan het toekomstige ERP-systeem worden gesteld. De functionele eisen worden vastgelegd in het Business Blueprint-document (kort: Business Blueprint).

In de ASAP-methode worden de functionele eisen gedefinieerd met behulp van op SAP R/3 toegesneden vragenlijsten (de zogenaamde Question & Answer Database (Q&A DB)). Het idee hiervan is dat SAP R/3-deskundige projectmedewerkers deze vragenlijsten door middel van interviews met eindgebruikers invullen. Een ingevulde vragenlijst moet een goed beeld geven van de oplossing in SAP R/3 en de vragenlijsten vormen de basis voor het genereren van het Business Blueprint-rapport.

In de Business Blueprint Phase moeten tevens discrepanties tussen de (huidige) bedrijfsvoering en de functionaliteit van het SAP R/3-systeem worden geïdentificeerd. Discrepanties hiertussen leiden ofwel tot het specificeren van aanvullende programmatuur (aanvullend maatwerk), ofwel tot wijzigingen in de bedrijfsprocessen.

Het Business Blueprint-document dient als basis voor de realisatie van het SAP R/3-systeem en dient formeel te worden geaccepteerd door de organisatie.

Realisation Phase
Het doel van de Realisation Phase is het implementeren (inrichten en programmeren) van de functionele eisen die zijn vastgelegd in het Business Blueprint-document. De implementatieconsultants richten in samenwerking met getrainde gebruikers van de organisatie het SAP-systeem in (in SAP R/3-termen 'customizen') volgens het Business Blueprint-document. Aan het einde van deze fase moet de inrichting van het SAP R/3-systeem en het programmeren van aanvullend maatwerk zijn afgerond en is het ERP-systeem door het projectteam getest.

Final Preparation Phase
Het doel van de Final Preparation Phase is het afronden van de laatste voorbereidingen voordat het ERP-systeem in productie wordt genomen, waaronder het uitvoeren van integratietests (in integratietests wordt het systeem als geheel en in samenhang met aanpalende systemen getest) door de gebruikersorganisatie, het opleiden van de eindgebruikers, het voorbereiden van het systeembeheer en het opstellen van een conversieplan. Daarnaast dient deze fase ook voor het afhandelen van de laatste belangrijke openstaande issues (issues zijn de problemen die tijdens het testen van het ERP-systeem naar voren zijn gekomen). Aan het einde van deze fase is het ERP-systeem klaar om in gebruik te worden genomen ('live' gaan).

Go Live & Support Phase
Het doel van de Go Live & Support Phase is het ERP-systeem op beheerste wijze in gebruik te nemen. Het ERP-systeem wordt in gebruik genomen en overgedragen aan een hiervoor toegesneden (staande) automatiseringsorganisatie. In de Go Live & Support Phase wordt onder andere aandacht besteed aan het inrichten van speciale ondersteuning voor de eerste kritische dagen na het 'live' gaan van het systeem. Deze ondersteuning is gericht op het beantwoorden van vragen die bij de beheerders en de gebruikers opkomen.

Daarnaast wordt de Go Live & Support Phase gebruikt om de ontwikkeling van het capaciteitsbeslag (gebruik) van het ERP-systeem te volgen en acties te nemen om de prestaties van het ERP-systeem te verbeteren.

Aan het einde van deze fase is het project afgesloten en overgedragen aan de staande organisatie.

ASAP Accelerators

Naast een projectfasering en WBS bieden projectmethoden als ASAP meestal een groot aantal hulpmiddelen (in ASAP-termen 'accelerators') die ondersteunen bij de projectuitvoering. Voorbeelden van deze accelerators in de ASAP-methode zijn: voorgedefinieerde projectplanningen in MS Project, hulpmiddelen om de benodigde SAP R/3-transacties (functionaliteit) te inventariseren, hulpmiddelen voor het testen van de inrichting en documentatie, en Business Blueprint-vragenlijsten in de Q&A DB.

AO/IC en ASAP

Om, als accountant, inzicht te verkrijgen in de wijzigingen in de maatregelen van AO/IC als gevolg van de introductie van een SAP R/3-systeem is het van belang een beeld te hebben van de mate waarin de ASAP-methode aandacht besteedt aan het implementeren van AO/IC-maatregelen.

De ASAP-methode bevat geen Work Packages en/of Activities die speciaal zijn gericht op het ontwikkelen van AO/IC. In de Project Preparation Phase, de Business

Blueprint Phase en de Realisation Phase van ASAP wordt in Activities wel (impliciet) aandacht besteed aan het ontwikkelen van maatregelen van AO/IC.

In de Project Preparation Phase wordt het belang van AO/IC onderkend bij het vertalen van de organisatiedoelstellingen naar kritische succesfactoren en meetindicatoren. Daarnaast is in de Business Blueprint Phase ruimte voor het beschrijven van de AO/IC (maatregelen van AO/IC dienen onderdeel te zijn van functionele eisen die worden gesteld aan het ERP-systeem en de bedrijfsprocessen). In de Project Preparation Phase en Final Preparation Phase wordt aandacht besteed aan de inrichting van algemene computercontroles, zoals scheiding van SAP R/3-omgevingen (in het SAP R/3-landschap), en inbedding van de SAP R/3-ontwikkel- en beheeraspecten in de staande ICT-ontwikkelings- en beheerorganisatie. Tot slot wordt in de Realisation Phase en Final Preparation Phase de logische toegangsbeveiliging van de SAP R/3-applicatie ingericht.

Geconcludeerd kan worden dat de ASAP-methode voldoende ruimte laat voor het ontwikkelen van AO/IC-beheersmaatregelen. Het projectmanagement dient echter zelf het belang van beheersmaatregelen te onderkennen en gestructureerd en met voldoende diepgang aandacht te schenken aan de ontwikkeling hiervan. Het projectmanagement dient het ontwerpproces van beheersmaatregelen te integreren met de ASAP-methode. Aangezien veel ERP-implementatiemethoden sterk overeenkomen met ASAP kan een overeenkomstige conclusie worden getrokken voor de meeste ERP-implementatiemethoden.

System Integration Controls

IRM heeft onderkend dat veel ERP-implementatiemethoden voldoende ruimte bieden, echter weinig concrete invulling geven aan het beoordelen, ontwerpen en ontwikkelen van ICT-beheersmaatregelen. IRM ziet hier een belangrijke taak weggelegd voor ICT-auditors. De ICT-auditor is namelijk gespecialiseerd in het identificeren van bedrijfsrisico's en vervolgens het beoordelen, ontwerpen en implementeren van ICT-beheersmaatregelen die deze risico's moeten afdekken.

De ASAP-methode bevat geen Work Packages en/of Activities die speciaal zijn gericht op het ontwikkelen van AO/IC.

Mede om bovengenoemde redenen heeft IRM de internationale SIC-methode ontwikkeld. De SIC-methode integreert een gestructureerde aanpak voor het beoordelen, ontwerpen en implementeren van ICT-beheersmaatregelen met projectmethoden (zoals ASAP) voor het implementeren van bedrijfsbrede informatiesystemen (waaronder ERP-systemen zoals SAP R/3) ([KPMG99]). In dit artikel wordt besproken op welke wijze de accountant deze SIC-methode kan inzetten. Hierna wordt de SIC-methode in meer detail besproken. Ingegaan wordt op de SIC-basismethode (in SIC-termen de 'Base Class'), de categorieën van ICT-beheersmaatregelen van de SIC-

System Integration Controls	Initiate	Assessment	Design	Implement	Follow-up & Evaluate	Close-out
Business Process Controls	**P-1** Prepare for Engagement **P-2** Prepare for Project **P-3** Define Project **P-4** Launch Project	**B-1** Assess Business Process Controls	**B-2** Design Business Process Controls	**B-3** Implement Business Process Controls	**B-4** Follow-up/ Evaluate Business Process Controls	**C-1** Close-out Project **C-2** Close-out Engagement
Infrastructure Security Controls	**P-1** Prepare for Engagement **P-2** Prepare for Project **P-3** Define Project **P-4** Launch Project	**S-1** Assess Infrastructure Security Controls	**S-3** Design Infrastructure Security Controls	**S-5** Implement Infrastructure Security Controls	**S-7** Follow-up/ Evaluate Infrastructure Security Controls	**C-1** Close-out Project **C-2** Close-out Engagement
Application Security Controls	**P-1** Prepare for Engagement **P-2** Prepare for Project **P-3** Define Project **P-4** Launch Project	**S-2** Assess Application Security Controls	**S-4** Design Application Security Controls	**S-6** Implement Application Security Controls	**S-8** Follow-up/ Evaluate Application Security Controls	**C-1** Close-out Project **C-2** Close-out Engagement
IT Operational Controls	**P-1** Prepare for Engagement **P-2** Prepare for Project **P-3** Define Project **P-4** Launch Project	**I-1** Assess IT Operational Controls	**I-2** Design IT Operational Controls	**I-3** Implement IT Operational Controls	**I-4** Follow-up/ Evaluate IT Operational Controls	**C-1** Close-out Project **C-2** Close-out Engagement
Data Conversion Controls	**P-1** Prepare for Engagement **P-2** Prepare for Project **P-3** Define Project **P-4** Launch Project	**D-1** Assess Data Conversion Controls	**D-3** Design Data Conversion Controls	**D-5** Implement Data Conversion Controls		**C-1** Close-out Project **C-2** Close-out Engagement
Data Interface Controls	**P-1** Prepare for Engagement **P-2** Prepare for Project **P-3** Define Project **P-4** Launch Project	**D-2** Assess Data Interface Controls	**D-4** Design Data Interface Controls	**D-6** Implement Data Interface Controls	**D-7** Follow-up/ Evaluate Data Interface Controls	**C-1** Close-out Project **C-2** Close-out Engagement

Figuur 3. SIC Base Class.

methode, de fasering van de SIC-methode en mogelijke SIC-opdrachtscenario's.

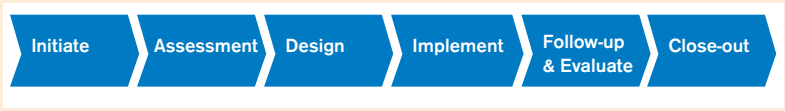
SIC Base Class

De SIC-methode bestaat uit een generieke basismethode (zie figuur 3) die kan worden ingezet voor alle bedrijfsbrede informatiesystemen. Daarnaast wordt deze basismethode aangepast op en uitgebreid voor specifieke versies van informatiesystemen, zoals JDEdwards, Baan, Oracle, Peoplesoft en SAP R/3. Onlangs heeft IRM de eerste pakketgerichte SIC-versie uitgebracht voor SAP R/3. Op korte termijn brengt IRM tevens pakketgerichte SIC-versies uit voor Peoplesoft en Oracle.

In de SIC SAP R/3-versie is de basismethode uitgebreid met een groot aantal SAP R/3-gerelateerde hulpmiddelen (normenkaders, pakketinformatie, plannen van aanpak, etc.). Hierbij is te denken aan de SAP R/3 Controls Database (een database met SAP R/3-specifieke risico's en beheersmaatregelen), de SAP R/3 Security Audit Approach (een aanpak voor het beoordelen van logische toegangsbeveiliging), verwijzingen naar websites, etc.

De SAP R/3-versie van de SIC-methode beschrijft de werkzaamheden die tijdens de levenscyclus van een SAP R/3-implementatieproject moeten worden uitgevoerd. Overeenkomstig ERP-implementatiemethoden, zoals ASAP, bestaat het raamwerk van de methode uit een WBS waarin individuele activiteiten zijn ondergebracht. Evenals in ASAP bestaat de WBS uit Tasks, Activities en Phases.

Fasen van de SIC-methode



Figuur 4. Fasering van de SIC-methode.

De SIC-methode is ontwikkeld met als doel gelijktijdig en geïntegreerd met standaard ERP-implementatiemethoden ICT-gerelateerde beheersmaatregelen te beoordelen, te ontwerpen en/of te implementeren. Om deze reden heeft de SIC-methode een fasering die sterk overeenkomt met de fasering van standaard ERP-implementatiemethoden, zoals ASAP. In tabel 1 is de fasering van de SIC-methode naast de fasering van de ASAP-methode gezet.

SIC-fasen	ASAP-fasen
1. Initiate	Project Preparation
2. Assessment	Business Blueprint
3. Design	Realisation
4. Implement	Final Preparation
5. Follow-up & Evaluate	Go Live & Support
6. Close-out	

Tabel 1. Fasen van de SIC- en de ASAP-methode.

Hierna worden de zes fasen van de SIC-methode besproken.

Initiate Phase
Het doel van de Initiate Phase is het SIC-project formeel te starten. Hiervoor wordt een projectplan opgesteld waarin onder andere de scope, aanpak en planning zijn vastgelegd. In de Initiate Phase is het van belang inzicht te verkrijgen in de organisatie (markt, bedrijfsvoering, ICT-infrastructuur, etc.). De fase bevat de volgende activiteiten:
* verkrijgen en beoordelen van achtergrondinformatie over de organisatie en het implementatieproject;
* definiëren van projectscope, aanpak en werkplannen voor de SIC-opdracht;
* verdeling van taken en verantwoordelijkheden tussen cliënt en het projectteam (accountant/ICT-auditor);
* definiëren van mijlpalen en rapportagerichtlijnen.

Assessment Phase
Het doel van de Assessment Phase is het beoordelen en/of vaststellen van de beheersmaatregelen die in en om het toekomstige ERP-systeem moeten worden geïmplementeerd. In de Assessment Phase worden de beheersmaatregelen geïnventariseerd die in de huidige processen en systemen zijn geïmplementeerd, wordt inzicht verkregen in het herontwerp van processen en wordt op basis van een risicoanalyse bepaald welke beheersmaatregelen de risico's moeten afdekken.

De Assessment Phase bevat de volgende activiteiten:
* verkrijgen van inzicht in de momenteel getroffen beheersmaatregelen in bedrijfsprocessen en systemen;
* verkrijgen van inzicht in nieuwe processen en maatregelen;
* evalueren van risico's en beheersmaatregelen;
* identificeren van de hiaten in de beheersing;
* formuleren van aanbevelingen ten aanzien van de beheersing (of definiëren van eisen aan beheersmaatregelen).

Design Phase
In de Design Phase worden beheersmaatregelen die in de Assessment Phase zijn gedefinieerd, vertaald naar technische specificaties voor de inrichting van het ERP-systeem. De specificaties worden overgedragen aan het implementatieteam, dat voorts het ERP-systeem conform specificaties inricht. De ontwerpfase bevat de volgende activiteiten:
* ontwikkelen van beheersmaatregelen;
* inventariseren van de SAP R/3-configuratie;
* specificeren van te ontwerpen beheersmaatregelen;
* communiceren omtrent specificaties van beheersmaatregelen met het implementatieteam.

Implement Phase
In de Implement Phase worden de beheersmaatregelen die in de Design Phase zijn ingericht, getest, eventueel aangepast en gedocumenteerd. Tot slot worden activiteiten geïdentificeerd die benodigd zijn om de beheersmaatregelen over te plaatsen naar de productieomgeving. Om goed te kunnen testen worden ter voorbereiding testcriteria en een testaanpak vastgesteld. De implementatiefase bevat de volgende activiteiten:
* definiëren van de testcriteria en testaanpak voor de beheersmaatregelen;
* testen van beheersmaatregelen;
* aanpassen/verbeteren van beheersmaatregelen;

* schrijven van definitieve documentatie van beheersmaatregelen;
* implementeren van beheersmaatregelen;
* overdragen van kennis aan cliënt.

Follow-up & Evaluate Phase
In de Follow-up & Evaluate Phase worden drie tot zes maanden na implementatie de geïmplementeerde beheersmaatregelen geëvalueerd. Eventueel worden aanbevelingen die in de tussentijd zijn geformuleerd, op basis van een post-implementation review opgevolgd. De Follow-up & Evaluate Phase bevat de volgende activiteiten:
* accorderen van geïmplementeerde beheersmaatregelen;
* beoordelen van de effectiviteit van de beheersmaatregelen;
* schrijven van een follow-up/evaluation-rapport.

Close-out Phase
De Close-out Phase heeft tot doel de SIC-opdracht formeel af te sluiten. Dit houdt in dat een definitieve rapportage wordt geschreven en overgedragen aan de cliënt. De Close-out Phase bevat de volgende activiteiten:
* schrijven van de definitieve rapportage;
* overdragen van de definitieve rapportage aan de cliënt;
* factureren en formele afsluiting;
* kennismanagement.

Categorieën van beheersmaatregelen

Ten behoeve van het beoordelen, ontwerpen en ontwikkelen van beheersmaatregelen in en om ERP-systemen onderscheidt de SIC-methode vier categorieën van ICT-gerelateerde beheersmaatregelen. Dit zijn de Business Process Controls, de Security Controls, de Data Integrity Controls en de IT Operational Controls. Hierna worden deze categorieën van beheersmaatregelen toegelicht.

Business Process Controls
Dit zijn beheersmaatregelen die in bedrijfsprocessen zijn getroffen om beheersing van de gegevensverwerking te waarborgen (hierbij is te denken aan waarborgen voor de betrouwbaarheid, continuïteit, effectiviteit en efficiëntie). Onderscheid wordt gemaakt tussen beheersmaatregelen in het ERP-systeem (de geprogrammeerde controles) en beheersmaatregelen rondom het ERP-systeem (de gebruikerscontroles). Voorbeelden van geprogrammeerde controles in SAP R/3 zijn kredietlimietcontroles, invoercontroles, en automatische toekenning van unieke nummerreeksen ([Kisj98]).

Security Controls
Dit betreft beheersmaatregelen die de logische en fysieke toegangsbeveiliging tot het ERP-systeem dienen te waarborgen. De Security Controls zijn onderverdeeld in de categorieën Infrastructure Security Controls en Application Security Controls.

Infrastructure Security Controls zijn gericht op de beveiligingsaspecten ten aanzien van de ICT-infrastructuur die is gerelateerd aan het ERP-systeem. De ICT-infrastructuur van een SAP R/3-systeem bestaat onder andere uit het bedrijfsnetwerk, de PC's van de eindgebruikers, het besturingssysteem van het systeem waarop de SAP R/3-applicatie is geïnstalleerd en het databasemanagementsysteem (DBMS) van de SAP R/3-applicatie. Beoordeling en/of ontwerp van Security Controls is daarom gericht op onder andere de beveiliging van het besturingssysteem, de beveiliging van het bedrijfsnetwerk en de beveiliging van het DBMS.

Application Security Controls zijn de beheersmaatregelen inzake toegangsbeveiliging gericht op de SAP R/3-applicatie zelf. Hierbij kan worden gedacht aan het inrichten van de autorisaties in de SAP R/3-applicatie of aan de wijze waarop de wachtwoordbeveiliging is ingericht (minimumaantal karakters van het wachtwoord, aantal keer dat een verkeerd wachtwoord kan worden ingegeven, etc.).

Data Integrity Controls
Dit zijn beheersmaatregelen die de blijvende betrouwbaarheid en beschikbaarheid moeten waarborgen van de gegevens in de database van het ERP-systeem. Data Integrity Controls zijn onderverdeeld in Data Conversion Controls en Data Interface Controls.

Data Conversion Controls zijn de beheersmaatregelen die de juistheid, volledigheid en controleerbaarheid van gegevensconversie dienen te waarborgen. Conversie van gegevens van de oude informatiesystemen naar het nieuwe ERP-systeem is in principe een eenmalige activiteit die wordt uitgevoerd ten behoeve van het in productie nemen van het ERP-systeem. Het beoordelen, het ontwerpen en/of het implementeren van Data Conversion Controls is bijvoorbeeld gericht op:
* de (geautomatiseerde) hulpmiddelen die worden gebruikt voor de gegevensconversie (zijn deze getest en geaccordeerd?);
* de verdeling van taken en verantwoordelijkheden ten aanzien van het uitvoeren van de gegevensconversie;
* de wijze waarop de (juistheid en volledigheid van) gegevensconversie wordt gecontroleerd en de wijze waarop deze controle wordt vastgelegd (controleerbaarheid).

Data Interface Controls zijn de beheersmaatregelen gericht op het waarborgen van de betrouwbaarheid, continuïteit, effectiviteit en efficiëntie van de geautomatiseerde interfaces van het ERP-systeem met andere informatiesystemen. Het beoordelen en/of ontwerpen van Data Interface Controls is bijvoorbeeld gericht op:
* de foutverslagen en loggings die worden gegenereerd door interfaceverwerking;
* het oplossen van fouten die optreden gedurende de interfaceverwerking;
* de wijze en frequentie waarop interfaceverwerkingen worden gestart (automatisch/handmatig).

IT Operational Controls
Dit zijn de algemene computercontroles (exclusief toegangsbeveiliging) die worden ingericht in de ontwikkelings- en beheerorganisatie van het toekomstige ERP-systeem. Hierbij valt te denken aan het inrichten van test-/acceptatie-/overdrachtsprocedures (change management) en het inrichten van procedures voor back-up en recovery.

SIC-scenario's

Door één, meerdere of alle SIC-fasen te combineren met één, meerdere of alle categorieën van beheersmaatregelen, kunnen verschillende opdrachtscenario's worden gevormd. In tabel 2 zijn vier typische SIC-scenario's toegelicht.

Scenario	Toelichting
End-to-end All Services	In deze adviesopdracht worden, gelijktijdig met het implementatieproject, alle SIC-fasen doorlopen om alle categorieën beheersmaatregelen te ontwerpen en te implementeren.
End-to-end Business Controls	In deze adviesopdracht worden, gelijktijdig met het implementatieproject, alle SIC-fasen doorlopen om de gebruikers- en geprogrammeerde controles (inclusief autorisaties) te ontwerpen en te implementeren.
Pre-/post-implementation Review	In deze auditopdracht worden, tijdens de SIC Initiate, Assessment en Implement Phase, de in opzet en bestaan getroffen beheersmaatregelen (alle categorieën) beoordeeld.
Pre-/post-implementation Security Review	In deze auditopdracht worden, tijdens de SIC Initiate, Assessment en Implement Phase, de in opzet en bestaan getroffen beheersmaatregelen ten behoeve van logische toegangsbeveiliging beoordeeld.

Tabel 2. Vier typische SIC-scenario's.

Onderscheid kan worden gemaakt, zoals blijkt uit tabel 2, tussen scenario's voor auditopdrachten en scenario's voor adviesopdrachten. Adviesopdrachten zijn gericht op het ontwerpen en/of implementeren van beheersmaatregelen in en om het ERP-systeem. Auditopdrachten zijn gericht op het beoordelen van beheersmaatregelen in opzet (Assessment Phase) en bestaan (Implement Phase).

Afhankelijk van het opdrachtscenario dat wordt geselecteerd, kunnen het aantal en de inhoud van de te doorlopen fasen van de SIC-methode verschillen. De Initiate Phase en Close-out Phase worden voor ieder denkbaar opdrachtscenario doorlopen. Per opdrachtscenario kunnen hierbij de omvang en de diepgang van de uit te voeren activiteiten verschillen. Voor een 'pre-implementation review' gericht op het beoordelen van Security Controls is minder kennis van de organisatie en een minder omvangrijk plan van aanpak vereist dan voor een 'end-to-end' opdrachtscenario waarbij alle categorieën van beheersmaatregelen worden ontwikkeld en geïmplementeerd.

De inhoud en het doel van de Assessment Phase verschillen eveneens voor advies- en auditopdrachten. De uitkomsten van deze fase vormen in een adviesopdracht de functionele beschrijving van de beheersmaatregelen die in en om het ERP-systeem moeten worden geïmplementeerd in de Realisation Phase. De uitkomsten van de Assessment Phase vormen in auditopdrachten de conclusie en aanbevelingen ten aanzien van de in opzet getroffen beheersmaatregelen. Het bestaan van getroffen beheersmaatregelen dient in auditopdrachten tijdens de Implement Phase te worden beoordeeld (in deze fase zijn de in opzet beschreven beheersmaatregelen geïmplementeerd in het ERP-systeem).

De Design Phase is hoofdzakelijk van toepassing op adviesopdrachten, omdat in deze fase de beheersmaatregelen worden geconfigureerd en/of geprogrammeerd in het ERP-systeem. Eventueel kan in een auditopdracht in de Design Phase de vertaling van functionele specificaties in technische specificaties worden beoordeeld.

De Implement Phase wordt met name doorlopen in het kader van adviesopdrachten. De Implement Phase kan in het kader van auditopdrachten worden gebruikt om te toetsen of de beheersmaatregelen die in de Assessment Phase in opzet zijn beschreven, volgens de specificatie (opzet) zijn geïmplementeerd in het ERP-systeem (bestaan).

De Follow-up & Evaluate Phase kan in auditopdrachten worden gebruikt om een post-implementatie review uit te voeren op de getroffen beheersmaatregelen in en om het ERP-systeem. Daarnaast kan tijdens de Follow-up & Evaluate Phase worden nagegaan of (in eerdere audits) gesignaleerde tekortkomingen zijn opgelost.

De SIC-methode toegepast voor (en door) accountants

Verscheidene opdrachtscenario's van de SIC-methode kunnen accountants (tezamen met een ICT-auditor) ondersteunen in het op gestructureerde wijze, en gelijktijdig met de projectuitvoering, beoordelen of inrichten van de beheersmaatregelen die in en rond het toekomstige ERP-systeem worden geïmplementeerd. De accountant kan (tezamen met een ICT-auditor), afhankelijk van het gekozen scenario, een audit- en/of adviesrol vervullen tijdens het ERP-implementatieproject. In een auditrol kan de accountant bijvoorbeeld tijdens de ASAP Business Blueprint Phase, de in opzet getroffen beheersmaatregelen beoordelen en daarover voor aanvang van de ASAP Realisation Phase adviseren. In een adviserende rol kan de accountant tijdens de ASAP Business Blueprint Phase de te treffen beheersmaatregelen definiëren, en vervolgens de cliënt ondersteunen bij het inrichten, testen en implementeren van de beheersmaatregelen tijdens de Realisation, Final Preparation en Go Live & Support Phase.

In een auditrol, die bestaat uit het beoordelen van getroffen beheersmaatregelen, zijn met name de SIC Initiate Phase en de Assessment Phase van belang, eventueel aangevuld met de Implement Phase. Binnen deze scenario's kan de accountant de audit verder afbakenen door te bepalen op welke categorieën van beheersmaatregelen (Business Process, IT Operations, Security of Data Integrity Controls) de audit is gericht. In tabel 3 zijn de auditscenario's aangegeven waarin de accountant kan participeren. Om te beschikken over de noodzakelijke ICT-kennis zal de accountant de SIC-opdrachtscenario's in samenwerking met een ICT-auditor uitvoeren. Van ieder scenario is aangegeven welke SIC-fasen en beheersmaatregelen zijn betrokken en voorts aan welke ASAP-fasen het scenario kan worden gekoppeld.

In de opdrachtscenario's die in de tabel zijn genoemd, ontwerpt en implementeert de cliënt de beheersmaatregelen. De accountant beoordeelt de in opzet getroffen beheersmaatregelen en adviseert hierover voordat de Assessment Phase is afgerond en de Design Phase start. Vervolgens kan de accountant het bestaan van de beheersmaatregelen die de cliënt in de Design Phase heeft ingericht, toetsen in de Implement Phase. Het voordeel van deze aanpak (pre-implementatie audit) is dat de aanbevelingen van de accountant al voordat het ERP-systeem wordt ingericht bekend zijn en derhalve eenvoudig kunnen worden meegenomen in de ASAP Realisation Phase van het ERP-implementatieproject. De rol van de accountant in deze scenario's draagt bij aan de kwaliteit van de toekomstige AO/IC en vroegtijdig inzicht in de wijzigingen in de controleaanpak.

SIC en Business Process Analysis

Veel accountants gebruiken de internationale Business Process Analysis (BPA)-methode van IRM bij het uitvoeren van procesgerichte audits op informatiesystemen ([Koed99]). BPA is echter naast succesvolle toepassing in post-implementatie audits BPA ook zeer geschikt voor het uitvoeren van pre-implementatie audits ([KPMG98]). Hoe verhoudt BPA zich tot SIC?

De BPA-methode onderscheidt de volgende fasen[1]:
* Strategic analysis;
* Documentation;
* Risk assessment;
* Identify controls & Residual risk.

Op basis van deze BPA-fasen is de relatie met SIC eenvoudig aan te geven. De elementen van de BPA-fase Strategic Analysis zijn terug te vinden in de Initiate Phase van SIC. De Documentation-fase van BPA komt overeen met het verkrijgen van inzicht in huidige/nieuwe processen en maatregelen in de SIC Assessment Phase. De BPA-fase Risk Assessment komt overeen met het evalueren van risico's en beheersmaatregelen in de SIC Assessment Phase. Tot slot komt de BPA-fase Identify controls & Residual risk overeen met het identificeren van hiaten en het formuleren van aanbevelingen in de Assessment Phase van SIC.

Een BPA pre-implementation beoordeling is daarom te definiëren als een SIC-scenario waarin de Initiate Phase en Assessment Phase (eventueel aangevuld met de Implement Phase) worden gecombineerd met Business Process Controls, Application Security Controls en Data Interface Controls. De overige categorieën van beheersmaatregelen (Infrastructure Security, IT Operations, Data Conversion) vallen buiten de reikwijdte van een BPA-onderzoek.

SIC-fasen	Beheersmaatregelen	ASAP-fasen	Toelichting
1 Initiate Assessment (Implement) Close-out	Business Process & Data Interface	Project Preparation & Business Blueprint	* Beoordeling van in opzet (en bestaan) getroffen gebruikers- en geprogrammeerde controles (inclusief interfaces en autorisaties)
2 Initiate Assessment (Implement) Close-out	IT Operations	Project Preparation & Final Preparation	* Beoordeling van in opzet (en bestaan) getroffen algemene computercontroles tijdens specificatiefase
3 Initiate Assessment (Implement) Close-out	Security	Project Preparation & Business Blueprint & Final Preparation	* Beoordeling van in opzet getroffen maatregelen voor logische toegangsbeveiliging
4 Initiate Assessment (Implement) Close-out	Data Conversion	Final Preparation	* Beoordeling van in opzet (en bestaan) getroffen maatregelen voor gegevensconversie
5 Initiate Assessment (Implement) Close-out	Alle categorieën van beheersmaatregelen	Project Preparation & Business Blueprint & Final Preparation	* Beoordelen van in opzet (en bestaan) getroffen beheersmaatregelen voor alle categorieën

Tabel 3. Auditscenario's waarin de accountant kan participeren.

Conclusie

Voor accountants kan het wenselijk zijn om als gevolg van de introductie van een ERP-systeem bij een cliënt na te gaan in hoeverre de geïmplementeerde maatregelen van AO/IC in en rondom het ERP-systeem de betrouwbaarheid en continuïteit van gegevensverwerking waarborgen. Om te voorkomen dat (vlak) na de introductie van het ERP-systeem aanvullende beheersmaatregelen moeten worden getroffen, kan de accountant (ondersteund door een ICT-auditor) ervoor kiezen al tijdens het implementatieproject de beheersmaatregelen te beoordelen. Op deze wijze kunnen de aanbevelingen van de accountant nog tijdens het inrichten/ontwikkelen van het ERP-systeem worden meegenomen. Voorts resulteert deze aanpak erin dat een kwalitatief betere AO/IC wordt gerealiseerd in en om het ERP-systeem en dat de accountant al vroegtijdig inzicht heeft in wijzigingen ten aanzien van de controleaanpak.

De System Integration Controls-methode van IRM biedt accountants (in samenwerking met ICT-auditors) verscheidene opdrachtscenario's om op gestructureerde wijze en geïntegreerd met de projectaanpak c.q. het projectteam van de organisatie, tijdens het implementatieproject de beheersmaatregelen te beoordelen (en/of hierover te adviseren). De SIC-methode maakt hierbij onderscheid in verschillende categorieën van beheersmaatregelen (Business Controls, IT Operations, Security en Data Integrity) en heeft een fasering die sterk overeenkomt met standaard ERP-implementatiemethoden. Voorts biedt de SIC-methode naast een gestructureerde aanpak verschillende pakketgerichte hulpmiddelen (normenkaders, pakketinformatie, plannen van aanpak, etc.) voor het uitvoeren van audit- en adviesopdrachtscenario's.

1) Voor een uitgebreide beschrijving van de BPA-methode en -fasering wordt verwezen naar het in deze Compact verschenen artikel *Business Process Analysis en de jaarrekeningcontrole; een praktijkcasus* van mw. drs. M.J.A. Koedijk RA.

Drs. ing. A.M. Meuldijk is werkzaam als IRM-specialist bij KPMG Information Risk Management. Zijn werkzaamheden zijn gericht op audit- en adviesdiensten op het gebied van Enterprise Resource Planning (ERP), waaronder System Integration Controls en Business Process Analysis. Daarnaast participeert hij in de ontwikkeling van producten en trainingen gerelateerd aan ERP-diensten en treedt hij op als docent van interne en externe cursussen.

Naast een gestructureerde aanpak moet de accountant tevens kunnen beschikken over de vereiste kennis van de ICT-objecten waarop de SIC-opdracht is gericht. Het ERP-systeem SAP R/3, dat als voorbeeld heeft gediend in dit artikel, is een zeer omvangrijk systeem met erg veel mogelijkheden voor Business Process, Security, IT Operations en Data Integrity Controls. De accountant zal daarom in SIC-opdrachten gezamenlijk optreden met een ICT-auditor die de noodzakelijke kennis van het informatiesysteem, ICT-auditing en de SIC-methode heeft.

Literatuur

[Kisj98]
A.W. Kisjes RE RA en drs. H. Wolters RE RA, *Interne controle maatregelen in en rondom SAP R/3 introductie*, De EDP-Auditor, nr. 2, 1998, p. 17-29.

[Koed99]
Mw. drs. M.J.A. Koedijk RA, *Van systeembeoordeling naar procesbeoordeling*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999, p. 10-19.

[Koed99a]
A. Koedijk en A. Verstelle, *ERP in bedrijf*, KPMG Management Consulting N.V., Uitgeverij Tutein Nolthenius, 's-Hertogenbosch 1999.

[KPMG98]
Business Process Analysis Methodology Guide, KPMG IRM, 1998.

[KPMG99]
System Integration Controls Methodology, KPMG Information Risk Management, *Version 1*, 1999.

[SAP99]
AcceleratedSAP Implementation Assistent, SAP AG, *Version 4.5B*, 1999.