Van systeembeoordeling naar procesbeoordeling

Mw. drs. M.J.A. Koedijk RA

De beoordeling van informatiesystemen heeft sinds de eerste voorzichtige stappen in de jaren zestig een evolutie doorgemaakt van een gegevensgerichte aanpak naar een procesgerichte aanpak. Werd de systeembeoordeling – of beter de procesbeoordeling – in de beginjaren slechts uitgevoerd in het kader van de jaarrekening, nu zijn deze beoordelingen zowel voor het management als voor de accountant noodzakelijke analyses met veel toegevoegde waarde. In deze inleiding wordt een overzicht gegeven van de ontwikkelingen op dit gebied.

Inleiding

In het midden van de jaren zestig werden in Nederland de eerste stappen gezet op het gebied van de beoordeling van informatiesystemen. Deze beoordelingen vonden voornamelijk plaats in het kader van de jaarrekeningcontrole. EDP-auditing bleek een vakgebied dat in de Verenigde Staten reeds enkele jaren in ontwikkeling was en dat in Nederland onder de term 'Automatisering en Controle' werd uitgewerkt door het NIVRA. In 1970 en 1975 werden de NIVRA-geschriften 1 (de invloed van de administratieve automatisering op de interne controle) en 13 (de invloed van de geautomatiseerde gegevensverwerking op de accountantscontrole) gepubliceerd. Vooral NIVRA-geschrift 13 heeft een belangrijke rol gespeeld in de ontwikkeling van de discussie rond systeemgericht (inclusief gebruikmaking van de in de automatisering opgenomen beheersmaatregelen) en gegevensgericht controleren ([KPMG86]).

Het duurt tot 1985 voordat in Compact nummer 40 een aanpak wordt gepubliceerd om de betrouwbaarheid van een geautomatiseerd informatiesysteem te beoordelen. Dit is de binnen KPMG ontwikkelde CASA-methode (Cursus Aanpak Systeembeoordeling en Accountantscontrole). In 1988 volgt het NIVRA met FASA (Feitelijke Aanpak System Audits), welke onder andere is gebaseerd op de CASA-methode, PRODOSTA (Project Control and Documentation Standards) en de Reliability control guidelines, die beide zijn ontwikkeld door Philips.

In 1996 wordt wederom in Compact de vernieuwde systeembeoordelingsaanpak van KPMG gepubliceerd, namelijk SRS (System Review Services).

In dit artikel worden samenvattingen gegeven van CASA en SRS. Daarnaast wordt naar aanleiding van ontwikkelingen in de jaren negentig en de voortdurende integratie van IT in de bedrijfsprocessen de nieuwe internationale KPMG-beoordelingsaanpak Business Process Analysis (BPA) beschreven.

Systeembeoordelingsmethoden

In deze paragraaf zal worden ingegaan op NIVRA-geschrift 13 en op de in de inleiding genoemde systeembeoordelingsmethoden die in de loop van de jaren zijn ontwikkeld en gebruikt in de praktijk.

NIVRA-geschrift 13

NIVRA-geschrift 13 ([NIVR75]) behandelt per element van het controleprogramma de invloed van automatisering van de informatieverzorging. Om uitspraken te kunnen doen omtrent de aanpak van de jaarrekeningcontrole wordt in het geschrift uitgegaan van een ideaalbeeld van de organisatie.

In het hoofdstuk beoordeling van de organisatie wordt het volgende gesteld:
'Bij goed opgezette geavanceerde toepassingen van computers kan de accountant in belangrijker mate dan voorheen gebruik maken van de waarborgen die het computersysteem in samenhang met de omringende organisatie biedt. Om daarvan te kunnen profiteren zal de accountant terdege moeten nagaan of het systeemontwerp aan alle daaraan uit een oogpunt van controle te stellen eisen voldoet.
Het desbetreffende onderzoek dient zich uit te strekken van de herkomst der basisgegevens af tot en met het gebruik dat intern van de geproduceerde informatie wordt gemaakt'.

Uit deze paragraaf blijkt dat het NIVRA reeds in 1975 van mening is dat de accountant gebruik kán maken van de waarborgen in en rondom het geautomatiseerde informatiesysteem. In de jaren negentig zien we de discussie dat de accountant in het kader van de controle van de jaarrekening niet meer buiten de beoordeling van de IT-risico's kan ([Munc95], [Heck97]).

In het NIVRA-geschrift wordt aangegeven aan welke elementen naast het systeemontwerp bijzondere aandacht moet worden geschonken. Dit zijn de gebruikersparticipatie bij systeemontwerp, het inbouwen van uitgebreide controlemaatregelen in de computerprogramma's, de aanwezigheid van goede documentatie, goede test-, acceptatie- en overdrachtsprocedures, de aanwezigheid van functiescheiding in de automatiseringsorganisatie en tussen de automatiseringsorganisatie en de operationele afdelingen, de toereikendheid van de managementinformatie en de opzet en werking van systeemontwikkelingsprojecten.

Geconcludeerd kan worden dat NIVRA-geschrift 13 de eerste aanzet in Nederland is om invulling te geven aan de beoordeling van de automatisering in het kader van de jaarrekeningcontrole. Onderscheid wordt hierbij gemaakt tussen algemene maatregelen en de geprogrammeerde controles. Met uitzondering van de algemene vragenlijsten die zijn opgenomen in de bijlagen wordt in het geschrift geen methode of aanpak beschreven om de geprogrammeerde maatregelen in kaart te brengen en hoe daarover een oordeel te vormen.

CASA

Cursus Aanpak Systeembeoordeling en Accountantscontrole (CASA) ([Koed85]) is een methode voor het beoordelen van de betrouwbaarheid van een (geautomatiseerd) informatiesysteem. Het betreft een in de praktijk ontstane, op een functionele benadering gebaseerde werkwijze die systematisch is uitgewerkt.

Afhankelijk van de situatie (bijvoorbeeld een onderzoek uitsluitend in het kader van de jaarrekeningcontrole of een specifieke opdracht) kunnen de breedte en diepgang van het onderzoek worden gevarieerd. Daarmee verschaft de CASA-methode de mogelijkheid in een aantal fasen verengingen aan te brengen.

De CASA-methode is ontworpen voor de algemene accountant, die naar 'heden ten dage mag worden verwacht' (1985!) wel over basiskennis van automatisering beschikt. Gebleken is dat de kennis van de accountant (met betrekking tot bedrijfsprocessen en de beheersing daarvan) bij het onderzoek van groter belang is dan de bij EDP-auditors aanwezige automatiseringskennis. De onontkoombare invloed van de techniek op de betrouwbaarheid noopt echter veelal wel tot de behoefte aan bijstand van de EDP-auditor. De CASA-methode kent duidelijke momenten, waarop de inbreng van een specialist gewenst/noodzakelijk zal kunnen zijn.

CASA is functioneel en top down. Dit wil zeggen dat niveaus van detaillering per 'functie' mogelijk zijn. Daarnaast wordt door de functionele benadering geabstraheerd van de technische uitwerking. Primair richt CASA zich op het beoordelen van de opzet en het bestaan van het systeem. De 'werking' wordt voorzover noodzakelijk getest.

De volgende fasen worden onderkend, waarbij de fasen IV tot en met VIII het daadwerkelijke systeemonderzoek betreffen:

I 'Understanding the business' en de systemen;
II Keuze van het te onderzoeken systeem (target systeem);
III Inventarisatie algemene maatregelen (in automatiseringsafdeling);
IV Inzicht verkrijgen in het te onderzoeken targetsysteem;
V Opstellen raamwerk van internecontrole-eisen;
VI Inventarisatie bestaand internecontrolestelsel;
VII Evaluatie internecontrolestelsel;
VIII Aanvullend onderzoek (opdracht aan EDP-auditor);
IX Opstellen/aanpassen controleprogramma;
X Uitvoeren controleprogramma.

'Vooronderzoek' (fase I tot en met III)
In de eerste twee fasen worden inzicht in en begrip van de organisatie, de bedrijfsprocessen en op hoog niveau van het informatiesysteem verkregen. Dit resulteert in inzicht op een conceptueel niveau van de gegevensverzamelingen en de informatiestromen tussen bedrijfsfuncties onderling en tussen bedrijfsfuncties en het informatiesysteem (het volledige stelsel van handmatige en geautomatiseerde applicaties).

In fase III vindt een eerste beoordeling plaats van de automatiseringsorganisatie en van de organisatie van de automatisering. Deze beoordeling moet aangeven of al dan niet een verhindering bestaat om een systeemgerichte controle inclusief een systeemonderzoek als controlebenadering toe te passen.

Inzicht verkrijgen in het te onderzoeken targetsysteem
In deze fase wordt een model (de opzet) van het geselecteerde applicatiesysteem vervaardigd voor de onderzoeker. Het systeem wordt als het ware geherdefinieerd, zodanig dat het model de 'te beheersen systeemfuncties' zichtbaar maakt. Deze herdefiniëring is noodzakelijk om een beoordeling door de accountant mogelijk te maken.

Inventarisatie en evaluatie internecontrolestelsel
Per eis worden de maatregelen geïnventariseerd, waarna wordt geëvalueerd of aan de eis wordt voldaan.

Als output kent CASA:
* rapport, inclusief oordeel en belangrijkste bevindingen en aanbevelingen;
* functioneel schema inclusief toelichting;
* raamwerk van internecontrole-eisen;
* inventarisatie en evaluatie (per controle-eis).

CASA is mede door de functionele benadering uitstekend toepasbaar bij systemen in ontwikkeling. De methode ondersteunt de accountant bij het participeren in de totstandkoming van het logisch ontwerp. Indien de accountant niet actief deelneemt aan het ontwikkelingsproces kunnen na gereedkoming van het logisch ontwerp de fasen IV en V van de CASA-methode worden uitgevoerd, mits de beschrijvingen van de gegevensverzamelingen bekend zijn. Daarna kan de accountant betrokken zijn bij het vertalen van de internecontrole-eisen naar concrete maatregelen.

CASA en FASA

In 1988 wordt het NIVRA-geschrift 44 ([NIVR88]) uitgegeven over FASA (Feitelijke Aanpak System Audits). Zoals al eerder aangegeven is FASA gebaseerd op de destijds bestaande methoden, zoals CASA en PRODOSTA (Project Control and Documentation Standards van Philips). De werkgroep FASA is van mening dat een combinatie van diverse methoden beter tegemoetkomt aan de gestelde eisen voor systeembeoordeling, hetgeen geresulteerd heeft in FASA.

FASA valt uiteen in twee gedeelten. Het eerste gedeelte is bedoeld voor het verkrijgen van een totaalbeeld van het te onderzoeken gebied, voor wat betreft de bedrijfsprocessen, bedrijfsrisico's en de vraag of de primaire registratie in voldoende mate is verzekerd. Aan de hand van de resultaten van deze fase wordt bepaald of een diepgaand onderzoek zinvol is.

In het tweede gedeelte wordt bepaald welk onderdeel nader moet worden onderzocht en hoe dat onderdeel het beste kan worden afgegrensd. Daarna vindt het feitelijke onderzoek plaats naar het geselecteerde onderdeel. De uit te voeren activiteiten in deze fase zijn:
* verzamelen van informatie omtrent de werkelijke gegevensverwerking van het geselecteerde gebied;
* indelen van de aanwezige gegevensbestanden naar mate van belang voor het onderzoek;
* groepering van de gegevenselementen per verantwoordelijke functionaris per bedrijfsproces en naar verwachte gelijkheid van de beheersmaatregelen;
* formuleren van controledoelstellingen per informatieverwerkende functie;
* inventariseren van de in opzet aanwezige controlemaatregelen per functie;
* toetsen op het bestaan van de controlemaatregelen;
* evaluatie.

FASA fase 1 komt overeen met de CASA fasen I en II en uit de beschrijving van de uit te voeren stappen in het NIVRA-geschrift blijkt dat in fase 2 gekozen is voor nagenoeg dezelfde aanpak als bij de CASA-methode. Dezelfde voorbeelden en uitwerkingen worden dan ook gebruikt. Bij FASA richt het onderzoek zich overigens alleen op *kritische* informatieverwerkende functies. Dit betekent dat na de keuze van het te onderzoeken bedrijfsproces nog steeds invulling is gegeven aan risicoanalyse en de top-downaanpak. Een ander verschil tussen CASA en FASA is dat FASA spreekt over bedrijfsprocessen en daarbij onderscheid maakt tussen handmatige activiteiten en activiteiten door/met het applicatiesysteem, terwijl CASA na het vooronderzoek zich richt op het targetsysteem.

SRS

System Review Services (SRS) ([Koed96]) wordt in 1996 in Compact gepresenteerd als een efficiënte methode om met behulp van een definitie van bedrijfsdoelstellingen en -risico's de betrouwbaarheid van een informatiesysteem te beoordelen. Hierbij wordt gebruikgemaakt van een sterk functioneel én procesgerichte benadering. Gesteld wordt dat gebruikers voor hun maatregelen van interne controle in toenemende mate afhankelijk zijn van automatisering, maar dat gebruikers vaak niet voldoende inzicht hebben in de wijze waarop een en ander wordt beheerst. Het gevolg kan zijn dat geautomatiseerde maatregelen verkeerd worden geïnterpreteerd, waardoor noodzakelijke gebruikerscontroles achterwege blijven of ten onrechte worden uitgevoerd.

Gezien de toenemende graad van automatisering van de bedrijfsprocessen en het koppelen (integreren) van logistieke systemen met de financiële applicaties is de accountant genoodzaakt inzicht te krijgen in de betrouwbaarheid van de kritieke informatiesystemen. Onvoldoende inzicht in en begrip van de functionaliteit van de systemen bij de cliënt kunnen daarbij de accountant ten onrechte tot een gegevensgerichte benadering dwingen.

SRS is geschikt voor gebruikers en de accountant met beperkte technische kennis om inzicht te krijgen in de betrouwbaarheid van geautomatiseerde systemen. Binnen KPMG is SRS de opvolger van CASA en geldt zij als de internationale systeembeoordelingsmethode.

Deze methode richt zich op de toepassingscontroles als het specifieke object van onderzoek. Deze toepassingscontroles betreffen zowel de geprogrammeerde als de gebruikerscontroles. Uiteraard wordt de relatie met de algemene computercontroles niet vergeten, maar gesteld wordt dat daarvoor andere onderzoeksmethoden zijn ontwikkeld.

Binnen SRS worden de volgende fasen onderscheiden:
1 opdrachtformulering;
2 'understanding the business';
3 'risk assessment';
4 'understanding the target system';
5 vaststellen eisen van interne controle;
6 inventarisatie en evaluatie van beheersmaatregelen;
7 rapportage.

In de fase van opdrachtformulering moet samen met de opdrachtgever helder in kaart worden gebracht wat het doel en object van het onderzoek, de scope (reikwijdte), de doorlooptijd, de verwachte kosten en het eindproduct (rapport) is. Tijdens de opdrachtformulering moet duidelijk worden welke (gedeelten van de) systemen zullen worden beoordeeld. Verder wordt beoordeeld of het onderzoek is beperkt tot een oordeel omtrent opzet en bestaan of dat de werking ook wordt meegenomen en wordt bepaald op welke kwaliteitsaspecten (betrouwbaarheid, effectiviteit en/of efficiency) het onderzoek zich richt.

Om tot een heldere definiëring van de scope te komen, kan het noodzakelijk zijn om eerst een vooronderzoek uit te voeren. Dit vooronderzoek zal in het algemeen de uitvoering van de fase 'understanding the business' inhouden.

Inzicht verkrijgen in het bedrijf en de markt waarin het opereert, is de uitkomst van de fase 'understanding the business'. Dit is noodzakelijk om een beter begrip te verkrijgen voor het belang en het biedt de basis voor het uitvoeren van de volgende fase. Naast inzicht in de management control (beheersstructuur), de bedrijfscultuur, de bedrijfsdoelstellingen en de kritieke succesfactoren van het bedrijf wordt inzicht verkregen in:
* de belangrijkste bedrijfsprocessen en informatieverwerkende processen;
* de procesdoelstellingen van de te beoordelen processen;
* de IT-omgeving;
* de afhankelijkheid van het bedrijf ten aanzien van de geautomatiseerde systemen gerelateerd aan:
  – de beschikbaarheid (van informatie);
  – de betrouwbaarheid (van informatie);
  – de effectiviteit (van informatie).

Uitgaande van de opgedane kennis in de vorige fase wordt geanalyseerd welke oorzaken ('risico's') kunnen bestaan die de realisatie van de bedrijfsdoelstellingen bedreigen. Het kunnen zowel interne als externe factoren zijn die fouten in de informatievoorziening veroorzaken. Van elk gedefinieerd risico wordt een inschatting gemaakt van de waarschijnlijkheid dat dit risico zich zal voordoen en de mogelijke impact die het risico heeft op de kwaliteit van de informatievoorziening.

'Understanding the target system' leidt tot een helder functioneel inzicht in wat het systeem doet en hoe het systeem werkt. Het doel van deze fase is om zodanig inzicht te verwerven in het targetsysteem dat in de volgende fase bij onderkende systeemfuncties en voor de vastgestelde risico's, eisen van interne controle kunnen worden gedefinieerd. In deze fase worden dus de getroffen beheersmaatregelen nog niet geïnventariseerd.

De te beheersen risico's uit de fase 'risk assessment' worden gerelateerd aan de onderkende systeemfuncties. Daarna worden per systeemfunctie de eisen van interne controle gedefinieerd. Hierbij gaat het niet om het beschrijven van mogelijke maatregelen. Er kunnen namelijk verschillende maatregelen (of combinaties daarvan) toereikend zijn. De eis moet dus op een zodanig niveau worden gedefinieerd dat de effectiviteit van de daadwerkelijk getroffen maatregelen daaraan getoetst kan worden.

Per eis van interne controle worden de geïmplementeerde maatregelen geïnventariseerd aan de hand van interviews, directe waarnemingen en eventueel beschikbare documentatie. Net zoals in de fase 'understanding the target system' is het van belang dat de inventarisatie wordt afgestemd om misinterpretaties te voorkomen. Bij de evaluatie van de aangetroffen maatregelen wordt vervolgens beoordeeld of deze toereikend zijn om de gedefinieerde risico's te beheersen. Met andere woorden, of op effectieve wijze wordt voldaan aan de gestelde eisen van interne controle.

De output van deze fase bestaat uit een vastlegging van alle aangetroffen maatregelen per eis en de uitkomst van de beoordeling van de toereikendheid daarvan. Indien de getroffen maatregelen als onvoldoende worden beoordeeld, dienen aanbevelingen ter verbetering te worden gedefinieerd.

SRS is ook inzetbaar bij systemen in ontwikkeling. In dat geval zal gebruik worden gemaakt van functionele specificaties en prototypes om voldoende inzicht te verkrijgen in het te beoordelen systeem.

Conclusies naar aanleiding van de beschreven systeembeoordelingsmethoden

CASA is in Nederland de eerste gepubliceerde systeembeoordelingsmethode voor het beoordelen van de betrouwbaarheid van een geautomatiseerd informatiesysteem. De methode is in de praktijk ontwikkeld ten behoeve van de accountantscontrole. In het vooronderzoek wordt inzicht verkregen in het bedrijf, de bedrijfsprocessen en op hoog niveau in het informatiesysteem. Aan de hand van een risicoanalyse wordt beoordeeld welke conceptuele gegevensverzamelingen voor de accountantscontrole van belang zijn en op basis daarvan wordt het targetsysteem voor het daadwerkelijke systeemonderzoek bepaald. Onderdeel van CASA (fase III) vormt de beoordeling van de algemene computercontroles om vast te stellen dat geen verhindering bestaat voor een systeemgerichte accountantscontrole.

Aan het in kaart brengen van het systeem wordt in CASA invulling gegeven door allereerst de inhoud van de hoofdbestanden te analyseren. Dit betekent dat vanuit de gegevensverzamelingen de gegevensstromen en daarna de systeemfuncties in kaart worden gebracht. In deze fase kiest CASA dus voor een bottom-upaanpak vanuit de gegevens en derhalve voor een gegevensgerichte aanpak. Het in de CASA-methode gedefinieerde begrip systeemfunctie wordt zowel door FASA (NIVRA-geschrift 44) als door SRS overgenomen en is naast de functionele benadering de kracht en het succes van de methode. Zowel CASA als SRS kent een functionele benadering en is inzetbaar bij operationele systemen en bij systemen in ontwikkeling.

SRS richt zich op de accountant en op bedrijfsrisico's.

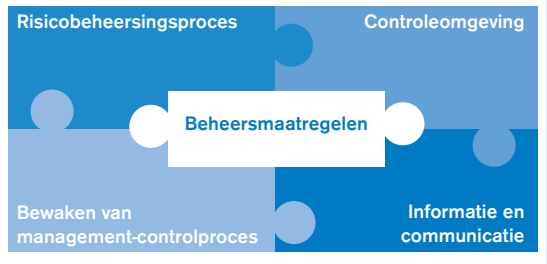
In 1996 wordt SRS gepresenteerd als een systeembeoordelingsaanpak die geschikt is voor de gebruikers en het management en óók voor de accountant. Het onderzoek richt zich daardoor niet (alleen) op de risico's voor de accountant, maar op de bedrijfsrisico's. Expliciet worden naast betrouwbaarheid, de aspecten efficiëntie en effectiviteit genoemd als mogelijke kwaliteitsaspecten waarop het onderzoek zich zal richten. In vergelijking met CASA wordt bij SRS de top-downbenadering met behulp van de risicoanalyse concreter gemaakt en wordt de relatie met het bedrijfsproces meer inhoud gegeven (hetgeen overigens bij FASA ook werd genoemd, maar in praktische zin niet is uitgewerkt). Dit laatste blijkt voornamelijk uit de fase 'understanding the target system', waar op basis van het bedrijfsproces de gegevensstromen en systeemfuncties in kaart worden gebracht in plaats van op basis van de gegevens zoals bij CASA.

Eisen aan de 'systeembeoordelingsmethode' van de 21ste eeuw

Gestelde eisen in het verleden

De eisen waaraan een systeembeoordelingsmethode moet voldoen, zijn volgens de werkgroep FASA als volgt uitgewerkt:

* effectiviteit;
* efficiëntie;
* praktisch, maar theoretisch gefundeerd;
* geschikt voor de jaarrekeningcontrole;
* geschikt om het onderzoek te faseren en af te grenzen;
* geschikt als onderzoeksmiddel;
* geschikt als vastleggingsmiddel;
* geschikt om andere deskundigen in te schakelen;
* geschikt om gegevens- of systeemgericht te controleren;
* geschikt om een ondersteuning te vormen voor dossiervorming;
* geschikt om de onderzoeksnormen vast te leggen en te beoordelen;
* geschikt om onafhankelijk van de graad van de automatisering een oordeel te kunnen vormen omtrent de betrouwbaarheid van de jaarrekening.



Figuur 1. De componenten van management control.

Ontwikkelingen in de jaren negentig

COSO

In september 1992 brengt het Committee of Sponsoring Organizations of the Treadway Commission (COSO) het rapport 'Internal Control - Integrated Framework' ([COSO92]) uit. In dit rapport wordt internal control gedefinieerd als een proces, ingesteld door het bestuur, het management of ander personeel, om redelijke zekerheid te verkrijgen over het behalen van de volgende doelstellingen:

- effectiviteit en efficiëntie van de bedrijfsprocessen (gericht op het behalen van de basisbedrijfsdoelstellingen, waaronder performance en winstdoelen en bescherming van activa);
- betrouwbaarheid van de financiële gegevens;
- naleving van de wetten en regelgeving.

De beheersing over deze gebieden kan ook worden omschreven als:

- operational control;
- financial control;
- compliance control.

Het management beschikt volgens het COSO-rapport over een vijftal onderling gerelateerde componenten voor het beheersen van de bedrijfsprocessen. Afhankelijk van allerlei factoren zoals grootte, type en cultuur van het bedrijf en de stijl van leidinggeven worden deze componenten door het management ingezet. Deze componenten van management control zijn:

- controleomgeving;
- risicobeheersingsproces;
- beheersmaatregelen;
- informatie en communicatie;
- bewaken van het management-controlproces.

De componenten van management control zijn onderling nauw verweven en vormen samen een geïntegreerd systeem. De componenten kunnen elkaar aanvullen, versterken, compenseren of verzwakken. Voor de beoordeling van de kwaliteit van de management control zullen de componenten dan ook in relatie tot elkaar moeten worden beoordeeld.

Het COSO-rapport heeft een belangrijke invloed gehad op de ontwikkelingen in de controleaanpak van de accountant en andere externe auditors. Mede omdat de discussie duidelijk heeft gemaakt dat de klanten meer van de accountants verwachten dan een uitspraak over de getrouwheid van de jaarrekening. Een voornamelijk gegevensgerichte controleaanpak waarbij de accountant zich slechts een beperkt beeld vormt van de management control binnen de organisatie, zal door een klant die toegevoegde waarde wenst van zijn accountant niet meer worden geaccepteerd. Al met al hebben het COSO-rapport en de discussies daarover ertoe geleid dat zowel interne als externe auditors zich nu meer richten op de interne beheersing van de bedrijfsrisico's en -processen en dat zij zich daarbij minder beperken tot dat ene kwaliteitsaspect betrouwbaarheid.

Het onderscheid tussen operational, financial en compliance control heeft geleid tot de ontwikkeling van drie verschillende 'audits', namelijk operational audit, financial audit en compliance audit. De bijbehorende beoordelingsmethoden zijn vaak los van elkaar ontwikkeld door verschillende disciplines (organisatieadviseurs, accountants en juristen) vanuit het kennisgebied van de betrokken discipline, maar 'raken' wel alle of bijna alle kwaliteitsaspecten. Zo is een operational audit met name gericht op effectiviteit en efficiency, maar wordt het aspect betrouwbaarheid vaak wel meegenomen. De vraag die hierbij gesteld moet worden, is natuurlijk of de verschillende methoden uitgevoerd door deskundigen uit verschillende disciplines wel leiden tot dezelfde uitspraak ten aanzien van een kwaliteitsaspect over een bepaald proces. Daarnaast rijst de vraag of de ondersteuning van het beoordeelde proces door het geautomatiseerde systeem in alle gevallen wel (voldoende) wordt meegenomen. Al met al pleit dit voor een procesbeoordelingsmethode die geschikt is voor de beoordeling van alle kwaliteitsaspecten door verschillende deskundigen (organisatieadviseurs, accountants, juristen, EDP-auditors) in een multidisciplinair team én waarbij de beoordeling van de procesondersteunende systemen een geïntegreerd onderdeel vormt van het onderzoek.

IT-auditing aangeduid

In het eerste NOREA-geschrift (juni 1998, [NORE98]) is de reikwijdte van het werkterrein van IT-auditing aangegeven aan de hand van een weergave van de domeinen die tot het vakgebied IT-auditing behoren. De studiegroep heeft daarbij de volgende domeinen en hun definities onderscheiden:

- *Informatiestrategie:* het geheel van doelstellingen, uitgangspunten en randvoorwaarden voor het omgaan met informatie binnen een organisatie en voor de organisatie van de informatievoorziening zelf.
- *IM/IT-management:* de door de leiding van een organisatie te scheppen voorwaarden voor de ontwikkeling, het beheer en het gebruik van geautomatiseerde systemen, alsmede de besturing van deze processen, zodanig dat de leiding kan vaststellen dat aan de door haar in de informatiestrategie geformuleerde doelstellingen en randvoorwaarden wordt voldaan.
- *Informatiesystemen:* de geautomatiseerde processen die primair ontworpen zijn om de mens te voorzien van gegevens, dan wel om de mens in staat te stellen de gegevens opgeslagen in computers – en overdraagbaar via datacommunicatietechnieken – te creëren, muteren, verwijderen, verspreiden en/of anderszins te manipuleren. Het geheel van organisatie en hulpmiddelen die primair dienen voor de ontwikkeling en het gebruik van informatiesystemen, behoort tevens tot het domein van informatiesystemen.
- *Technische systemen:* systemen die ontworpen zijn om geïmplementeerd te worden in hardware en systeemprogrammatuur met het doel de hardware en/of

(andere systeem)programmatuur aan te sturen. Technische systemen ondersteunen de geautomatiseerde processen binnen de informatiesystemen en processystemen door het aansturen en geautomatiseerd beheersen van de hardware die deel uitmaakt van de technische infrastructuur.

* *Processystemen:* systemen die ontworpen zijn om elektronische interfaces en daarmee apparaten (robots) aan te sturen. Het zijn geen informatiesystemen, omdat de systemen niet primair zijn ontworpen om de mens te ondersteunen met het verwerken van gegevens, maar om andere apparaten aan te sturen. Tot het domein van processystemen behoren tevens alle organisaties met een primaire verantwoordelijkheid voor deze systemen, alsmede de daarbij gebruikte hulpmiddelen.
* *Operationele automatiseringsondersteuning:* alle activiteiten van een organisatie die gericht zijn op het beheren en beschikbaar houden van de technische infrastructuur en de onder beheer zijnde IT-processen conform de afgesproken standaarden en service level agreements, alsmede de administratie daarvan. De operationele automatiseringsondersteuning van het organisatieonderdeel betreft de installatie, het beheer en het onderhoud van de automatiseringsmiddelen die ter beschikking staan van het organisatieonderdeel (inclusief de geleverde programmatuur).

Uit bovenstaande definities blijkt dat het domein van de informatiesystemen het object van onderzoek is voor de traditionele en ook voor de toekomstige systeem- of procesbeoordeling. Naast het informatiesysteem op zich wordt ook de organisatie tot het domein gerekend, evenals de ontwikkeling van het informatiesysteem. Dus niet alleen een bestaand informatiesysteem (inclusief het proces) is een IT-auditdomein, maar ook het ontwikkelingsproces. Een moderne systeembeoordelingsmethode dient daarom ingezet te kunnen worden bij zowel bestaande informatiesystemen als systemen in ontwikkeling. In het geschrift komt dit tot uiting in de volgende gedefinieerde objecten (naast de meer organisatorische objecten):

1 *eisen aan het informatiesysteem*. Het informatiebeleid en het beveiligingsbeleid en de daaruit voortvloeiende documenten dienen als normen voor de toetsing van de toereikendheid van de eisen die gesteld worden aan het te ontwikkelen informatiesysteem. Deze eisen kunnen tevens voortvloeien uit externe wet- en regelgeving. Daarnaast wordt beoordeeld in hoeverre de eisen zijn vertaald in maatregelen (interne controle) binnen en buiten de informatiesystemen.
2 *operationeel gebruik*. Informatiesystemen in gebruik kunnen onderwerp van beoordeling zijn, mits de general controls in de operationele ondersteuningsorganisaties toereikend zijn.

Opvallend is dat de eisen aan het informatiesysteem voortkomen uit het informatie- en beveiligingsbeleid en niet uit het organisatiebeleid. Wel wordt gesteld dat een goed informatiebeleid aansluit op de doelstellingen van de organisatie. Ook wordt conform het COSO-rapport het aspect wet- en regelgeving genoemd.

In het derde hoofdstuk van het geschrift worden de (mogelijke) kwaliteitsaspecten beschreven, namelijk:

* effectiviteit;
* efficiëntie;
* exclusiviteit;
* integriteit;
* controleerbaarheid;
* continuïteit;
* beheersbaarheid.

Bij de eerder beschreven systeembeoordelingsmethoden vormen exclusiviteit, integriteit en controleerbaarheid samen het aspect betrouwbaarheid. In vergelijking met SRS zijn continuïteit en beheersbaarheid nieuwe kwaliteitsaspecten die in het kader van de beoordeling van een systeem worden genoemd.

Eisen aan de 'nieuwe' methode

Uit bovenstaande ontwikkelingen kan worden afgeleid dat naast de eisen die zijn opgesomd in het NIVRA-geschrift 44 (FASA) de beoordelingsmethoden van de toekomst moeten voldoen aan de volgende eisen:

1 gericht op de beoordeling van een bedrijfsproces inclusief de IT-ondersteuning van dat proces (in plaats van 'alleen' proces- of 'alleen' systeemgericht);
2 gericht op de beheersing van bedrijfsdoelstellingen en daaruit voortvloeiende risico's met betrekking tot de kwaliteitsaspecten zoals deze in het COSO-rapport zijn genoemd; hetgeen betekent dat deskundigen uit verschillende disciplines dezelfde methode moeten kunnen gebruiken.

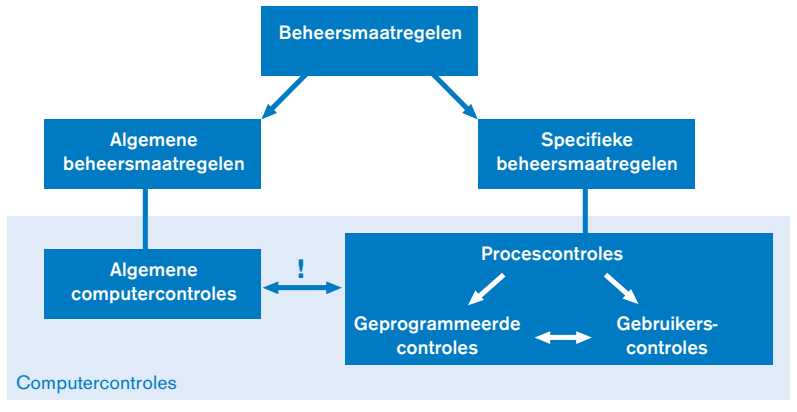
Daarnaast kan worden gesteld dat de methode geschikt moet zijn zowel voor processen/systemen in ontwikkeling als voor operationele processen. Tevens dient de methode consistent, flexibel en top down te zijn.

Business Process Analysis (BPA)

Uitgangspunten

Ontwikkelingen zoals in gang gezet door het COSO-rapport en de voortgaande ondersteuning van processen door IT, veroorzaken een aanscherping van de systeembeoordelingsmethode SRS. De opvolger van SRS is Business Process Analysis (BPA), een procesbeoordelingsmethode die het mogelijk maakt een bedrijfsproces te beoordelen inclusief het procesondersteunende informatiesysteem (of -systemen). 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.

BPA beoordeelt het proces én het informatiesysteem.



Figuur 2. Beheersmaatregelen.

BPA is geschikt voor de beoordeling van de betrouwbaarheid, de effectiviteit en efficiëntie en de compliancy van een proces. Hierbij is het wel van belang dat degene die de beoordeling uitvoert deskundig is op het vakgebied waarvan het kwaliteitsaspect wordt onderzocht. Indien alle kwaliteitsaspecten tot de scope van het onderzoek behoren is het mijns inziens noodzakelijk dat een multidisciplinair team van accountants, EDP-auditors, organisatieadviseurs en eventueel juristen de beoordeling uitvoert.

Zoals hiervoor is gebleken zal het management beheersmaatregelen invoeren die gerelateerd zijn aan operational, financial en compliance control. Dit zullen zowel algemene beheersmaatregelen zijn die gelden voor alle bedrijfsprocessen, als specifieke maatregelen in een proces. In verband hiermee is het management ook genoodzaakt beheersmaatregelen in te voeren die gebaseerd zijn op de specifieke risico's van IT, welke zijn onderkend bij de risicoanalyse. De risico's op het gebied van de informatie- en communicatiesystemen worden beheerst door computercontroles met een algemeen karakter (algemene computercontroles) en controles die zich richten op een specifiek proces, inclusief het procesondersteunende systeem, de zogenaamde toepassings- of procescontroles. Deze procescontroles bestaan uit zowel geprogrammeerde als gebruikerscontroles (figuur 2, [Munc95]).

De algemene computercontroles scheppen het kader dat ervoor moet zorgen dat de procescontroles effectief worden opgezet en dat de werking in de tijd van de geprogrammeerde procescontroles wordt gerealiseerd. De goede werking van de geprogrammeerde controles in een applicatie is bijvoorbeeld afhankelijk van de kwaliteit van de test-, acceptatie- en overdrachtsprocedures, die onderdeel zijn van de algemene computercontroles.

Het specifieke object van onderzoek van BPA zijn de procescontroles. Het feit dat de werking van deze controles in de tijd voor een (steeds groter) deel afhankelijk is van de algemene computercontroles zal veel auditors doen besluiten ook de algemene computercontroles te beoordelen. Hiervoor bestaan echter andere methoden en hulpmiddelen, zoals standaardvragenlijsten.

Als output kent BPA naast het rapport een processchema en de zogenaamde BPA-matrix (figuur 3).

BPA is niet alleen inzetbaar bij operationele processen, maar ook bij processen en systemen in ontwikkeling (meer adviesgericht).

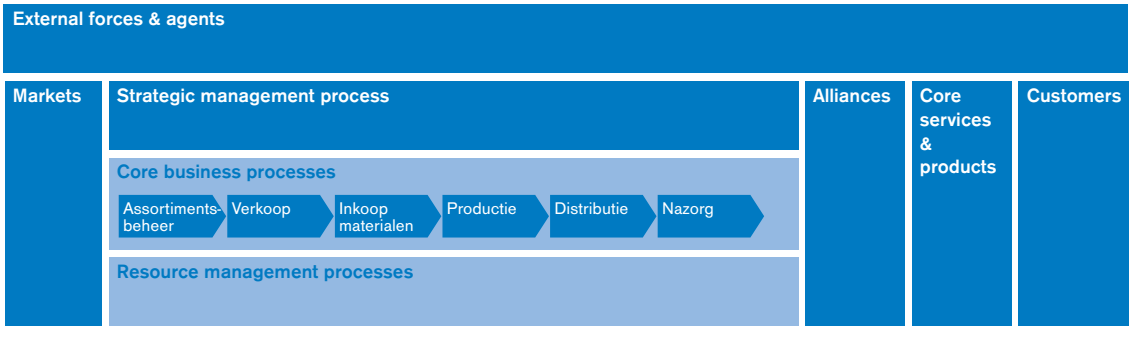
Fasering

BPA kent de volgende fasering:
1 Strategic analysis;
2 Documentation;
3 Risk assessment;
4 Identify controls;
5 Assess residual risk;
6 Test controls.

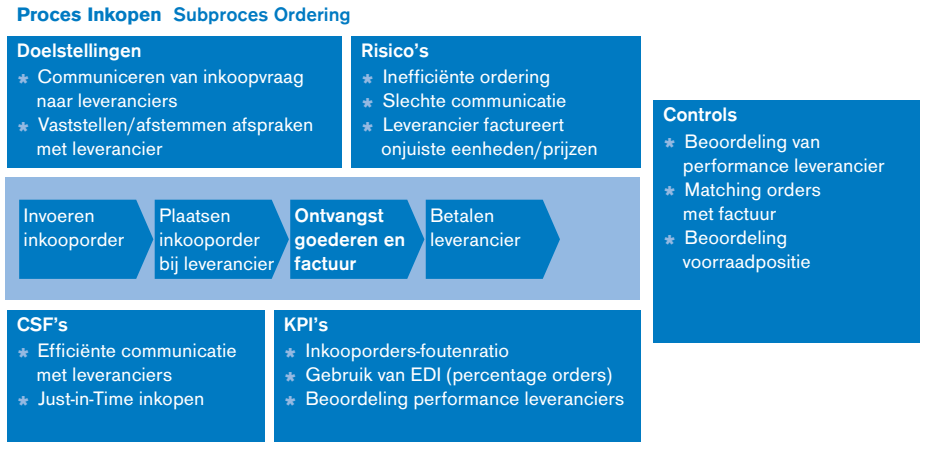
De fasen 2 tot en met 5 worden hierbij gezien als de procesanalyse. De opdrachtformulering en rapportage worden in BPA niet gezien als onderdeel van de methodologie, omdat deze onderdelen als standaardelementen van een IT-audit worden onderkend. Uiteraard vormen zij wel het begin en het eind van het onderzoek en staat het belang van een goede opdrachtformulering en rapportage voorop.

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

Figuur 3. BPA-matrix.



Figuur 4. Output Strategic analysis: business model.



Figuur 5. Output Strategic analysis (eerste procesanalyse).

Strategische analyse

Conform de fase 'understanding the business' van SRS of het vooronderzoek van CASA zal de beoordelaar in deze fase inzicht verkrijgen in het bedrijf, de strategie, de bedrijfsrisico's en doelstellingen, de bedrijfsprocessen en in de IT-omgeving. Deze informatie is noodzakelijk om de context van het onderzoek te doorgronden (waaronder het belang) en om het onderzoek te kunnen richten op de bedrijfsdoelstellingen en risico's, waardoor beter voldaan wordt aan de verwachtingen van de klant. Daarnaast is de opgedane kennis in deze fase het uitgangspunt voor de diepgang van het onderzoek.

Als eerste hulpmiddel kan de beoordelaar gebruikmaken van het zogenaamde business model, zoals dat is weergegeven in figuur 4. Andere hulpmiddelen/methoden die gebruikt kunnen worden, zijn bijvoorbeeld Porters PEST-analyse en de FIVE FORCES-analyse, hetgeen afhankelijk is van de in de opdrachtformulering gestelde doelstelling en kwaliteitseisen.

Naast de aspecten die in het bedrijfsmodel zijn opgenomen, zal de beoordelaar ten minste voor het te beoordelen proces informatie vergaren over de subprocessen, de procesdoelstellingen, de risico's en getroffen maatregelen (high level controls), de Key Performance Indicators (KPI's) en de Critical Success Factors (CSF's).

In figuur 5 wordt een voorbeeld gegeven van een uitwerking van de eerste analyse van het te beoordelen proces in de Strategic analysis-fase.

Fase Documentation

De fase Documentation van BPA vertoont veel gelijkenis met de fase inzicht in het informatiesysteem van SRS. Belangrijk is dat bij BPA de processtappen of activiteiten (inclusief mogelijke handmatige handelingen!) in kaart worden gebracht.

In de documentatiefase worden de volgende stappen uitgevoerd:
1 analyseren gegevensstromen (input/output-proces);
2 identificeren van activiteiten;
3 maken schema met toelichting en invullen matrix;
4 verificatie.

Uit de analyse van de gegevensstromen komen 'vanzelf' de te onderkennen activiteiten naar voren. Activiteiten worden hierbij gedefinieerd als het geheel van logisch bij elkaar behorende gegevensverwerkende activiteiten en/of transacties, al dan niet geautomatiseerd, en komen vaak overeen met een processtap.

De volgende soorten activiteiten worden binnen BPA onderkend:
1 bijwerken gegevensgroepen in bestanden (volgt uit analyse van gegevensstromen):
   – transacties op variabele gegevens,
   – mutaties op vaste gegevens;
2 uitvoeren reken- en beslissingsregels:
   – gegevensstroom door computer gegenereerde transacties (bijvoorbeeld: prolongatie, geautomatiseerde accordering);
3 handmatige activiteit:
   – processtap uitgevoerd door een functionaris buiten het procesondersteunende systeem om.

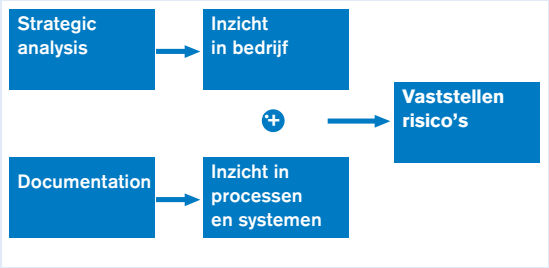
Het vastleggen van het proces in een schema wordt door de BPA-methodiek sterk aanbevolen omdat dit het inzicht in het proces vergroot. Een specifieke schematechniek schrijft BPA niet voor.

Uiteraard moet een uitgebreide verificatie plaatsvinden met de betrokken functionarissen en deskundigen, waarna tot slot de uitkomsten worden vastgelegd in de BPA-matrix. Deze matrix zal in de volgende fasen worden gecompleteerd (figuur 6).

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

*) Afhankelijk van verwachte beheersmaatregelen wordt een proces uitgesplitst in activiteiten

Figuur 6. BPA-matrix Documentation-fase.



Figuur 7. Vaststellen te beheersen risico's.

Risk assessment

In de Risk assessment-fase moeten de drie kolommen bedrijfsrisico's, risico-inschatting en normen van de BPA-matrix worden ingevuld. Allereerst worden per onderkende activiteit de bedrijfsrisico's vastgesteld, waarbij uiteraard de opgedane kennis in de fase Strategic analysis wordt meegenomen (zie figuur 7).

Vervolgens wordt een inschatting gemaakt van de hoogte van het risico. Deze risico-inschatting is een combinatie van de kans dat een risico zich voordoet en de impact daarvan (zie figuur 8). Bij het inschatten van de hoogte van het risico moet worden geabstraheerd van eventuele beheersmaatregelen die zijn getroffen (en waarvan de auditor mogelijk reeds op de hoogte is). We hebben het dus over het zogenaamde 'inherente' risico. Bij de beoordeling van de impact moet uiteraard rekening gehouden worden met de uitkomsten uit de Strategic analysis, waaronder met name de CSF's en KPI's.

Na de risico-inschatting worden per activiteit de normen of eisen van management control vastgesteld. Hierbij gaat het (conform SRS) niet om het beschrijven van de vereiste maatregelen, omdat verschillende beheersmaatregelen of combinaties daarvan toereikend kunnen zijn. Het is aan de auditor in de volgende fasen om in kaart te brengen welke maatregelen daadwerkelijk zijn getroffen om een bedrijfsrisico te beheersen en te beoordelen of deze mix van maatregelen effectief en efficiënt is.

Een voorbeeld:
De activiteit 'muteren kortingen' is onderkend in een handelsorganisatie. In overleg met het management is het volgende bedrijfsrisico vastgesteld: het missen van opbrengsten door het verlenen van te hoge kortingen. De risico-inschatting voor dit bedrijfsrisico is hoog. De kortingen worden vastgesteld per klant en de omzet per klant is aanzienlijk, waardoor de impact van een verkeerde korting significant is en het voorkomen is ingeschat op 'mogelijk'. De auditor heeft vervolgens de volgende eis van management control vastgesteld: hoge mate van zekerheid over autorisatie, tijdigheid en juistheid van de activiteit 'muteren kortingen'.

Identify controls en Assess residual risk

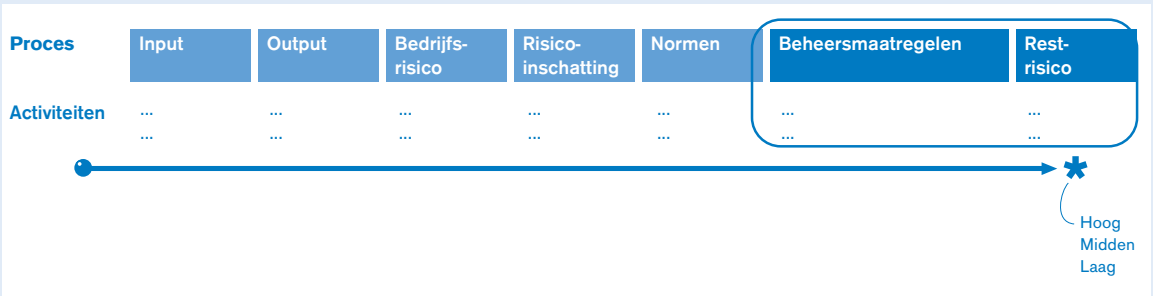
Voor elke norm zal de auditor vaststellen aan de hand van documentatie, waarnemingen en interviews welke beheersmaatregelen daadwerkelijk door het management zijn getroffen. Dit betreffen, zoals eerder reeds gezegd, de zogenaamde procescontroles en dus zowel de geprogrammeerde controles als de handmatige gebruikerscontroles. Uiteraard is verificatie ook bij deze fase een vast onderdeel.

Nadat de geïdentificeerde beheersmaatregelen zijn vastgelegd in de BPA-matrix zal de auditor het restrisico bepalen (figuur 9). Hierbij stelt de auditor vast of de getroffen beheersmaatregelen (inclusief de high level controls!) toereikend zijn om het risico te beheersen. Naast het bepalen van het restrisico zal de auditor analyseren of de gekozen mix van maatregelen wel een efficiënte mix is. Bij de beoordeling van de effectiviteit en efficiëntie van de mix van beheersmaatregelen zal de auditor bijvoorbeeld afwegen of een juist evenwicht bestaat tussen preventieve maatregelen en maatregelen achteraf, en tussen handmatige en geautomatiseerde controles. Vanzelfsprekend zal de auditor aanbevelingen ter verbetering formuleren als bovenstaande beoordelingen daar aanleiding toe geven.

Op verzoek van de klant of in het kader van de jaarrekeningcontrole kan het nodig zijn om de werking van de maatregelen te testen. Voor de werking van de geprogrammeerde controles bestaat hierbij een relatie met de algemene computercontroles, en dan vooral ten aanzien van de TAO-procedures en de logische toegangsbeveiliging. De algemene computercontroles zullen dan ook moeten worden beoordeeld om een uitspraak te kunnen doen over de werking van de geprogrammeerde controles. De gebruikerscontroles kunnen zoals thans gebruikelijk worden getest.

Voorkomen	Impact Niet significant	Gemiddeld	Significant
Waarschijnlijk	Middel	Hoog	Hoog
Mogelijk	Laag	Middel	Hoog
Onwaarschijnlijk	Laag	Laag	Middel

Figuur 8. Risicotabel.



Figuur 9. Identify controls and Assess residual risk.

De accountant zal aan de hand van de uitkomsten van de procesbeoordeling zijn controleprogramma moeten opstellen. Hiertoe zal de accountant allereerst moeten vaststellen in hoeverre de onderkende bedrijfsrisico's de getrouwheid van de jaarrekening raken om vervolgens aan de hand van de restrisico's (of in accountantstermen: internecontrolerisico's) te beslissen of puur systeemgericht gecontroleerd kan worden (restrisico laag) of dat naast de systeemgerichte controle aanvullende gegevensgerichte controles noodzakelijk zijn (restrisico middel of hoog).

Conclusie

Ontwikkelingen zoals in gang gezet door het COSO-rapport en de voortgaande ondersteuning van processen door IT veroorzaken een aanscherping van de systeembeoordelingsmethode SRS, zoals deze in 1996 in Compact is gepresenteerd. De opvolger van SRS is Business Process Analysis, een procesbeoordelingsmethode die het mogelijk maakt een bedrijfsproces te beoordelen inclusief het procesondersteunende informatiesysteem (of -systemen).

BPA is daarbij geschikt voor de beoordeling van zowel de betrouwbaarheid, de effectiviteit, de efficiëntie en de compliance van een proces. Hierbij is het van belang dat degene die de beoordeling uitvoert deskundig is op het betreffende vakgebied van het tot de scope behorende kwaliteitsaspect. Indien alle kwaliteitsaspecten tot de scope van het onderzoek behoren is het noodzakelijk dat een multidisciplinair team van accountants, EDP-auditors, organisatieadviseurs en eventueel juristen de beoordeling uitvoert.

BPA kent conform CASA en SRS een sterk gefaseerde en functionele methode, zodat gebruikers en accountants met een beperkte technische kennis met de beoordelingsmethode en de uitkomsten daarvan overweg kunnen. Het in de CASA-methode gedefinieerde begrip systeemfunctie dat zowel door FASA als SRS is overgenomen, is naast de functionele benadering de kracht en het succes van de methode. De kern van het begrip systeemfunctie wordt dan ook gehandhaafd bij BPA.

Literatuur

[COSO92]
COSO, Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*, AICPA 1992.

[Heck97]
E.F. Heck, M.J.A. Koedijk en W.A. de Munck, *Informatietechnologie en management control in het algemeen en voor het MKB in het bijzonder*, Compact 1997/4.

[Koed85]
A.H.C. Koedijk, *Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: De CASA methode*, Compact 1985/4.

[Koed96]
M.J.A. Koedijk, W.A. de Munck, *System Review Services*, Compact 1996/3.

[KPMG86]
Prof. D. Steeman, *Ontwikkeling EDP-audit in het kader van de jaarrekeningcontrole*, in: 24 over EDP Auditing, 1986.

[KPMG98]
Business Process Analysis, Methodology Guide.

[Munc95]
W.A. de Munck, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering* Compact 1995/3.

[NIVR75]
NIVRA-geschrift 13, *Automatisering en Controle; de invloed van de geautomatiseerde gegevensverwerking op de accountantscontrole*, 1975.

[NIVR88]
NIVRA-geschrift 44, *Automatisering en Controle; Feitelijke Aanpak Systems Audit*, 1988.

[NORE98]
NOREA-geschrift 1, *IT-auditing aangeduid*, 1998.