COMPACT

TIJDSCHRIFT EDP-AUDITING

ACCOUNTANTSCONTROLE EN IT

1996/3

Compact ®
Jaargang 23, nummer 3
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers RE
Drs. R.G.A. Fijneman RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
J.H. Buisman RA
Mr. P. van Dijken
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning,
Samsom Bedrijfsinformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 746
Fax : 0172 – 466 569
Vormgeving
Bureau Karakter, Delft
Opmaak
Sander Pinkse Boekproduktie, Amsterdam
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom Bedrijfsinformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij het redactiesecretariaat. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
Drs. ing. O.A. Rouwendal

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiserings-organisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

Een typisch voor de accountant geschreven nummer, dit nummer 96/3 van Compact. Niet zonder reden laat de redactie aan het einde van de voorjaarsdrukte en aan de vooravond van de interimcontroles een publikatie voor deze doelgroep verschijnen. U gaat nog op vakantie? Dit nummer is verplichte literatuur: het handelt over System Review Services ofwel het beoordelen van de betrouwbaarheid van informatiesystemen. Nauw daarmee verwant is de fiscale bewaarplicht van gegevens. De fiscus is met de ontwikkelingen in informatietechnologie meegegaan en heeft invulling gegeven aan de bewaarplicht in relatie tot elektronische opslag van gegevens.

Voor organisaties waar sprake is van vergaande integratie van processen is het van belang dat de functie- en taakverdeling wordt verankerd in systeemsoftware. Dit geldt niet slechts voor eindgebruikers, ook functiescheiding en procedures in de automatiseringsorganisatie dienen op een adequate wijze geautomatiseerd te worden ondersteund, opdat de eindgebruiker kan steunen op de kwaliteit ervan. De auteur licht de problematiek op een zodanige wijze toe dat de accountant zich realiseert tot welk punt zijn kennis reikt en dus ook: wanneer een EDP-auditor in te schakelen?

System Review Services (SRS), beschreven door twee auteurs van KPMG EDP Auditors-huize, behandelt een vernieuwde methode om de kwaliteit te beoordelen van de application controls. Vanzelfsprekend wordt veel aandacht besteed aan de aanpak van zo'n onderzoek.
Tot slot een artikel met als titel 'De EDP-auditor: vertrouwensman, agent of ...?' Het onderwerp – Agency-theorie – staat thans nogal in de schijnwerpers, doch het werd nog niet eerder geplaatst in de context van de EDP-auditor. Overigens behandelt de auteur het onderwerp niet dan nadat hij 'Limperg en de vertrouwenstheorie' heeft geanalyseerd en ook de Management Control-benadering heeft uitgewerkt.

De redactie wenst u een combinatie van leesplezier (permanente educatie-punten) en fijne vakantie.

Prof. A.W. Neisingh RE RA

Systeemsoftware onder controle

Drs. R.H.H.M. Bronzwaer

Onder deze stellige titel heeft de auteur enkele concepten neergezet waarmee een organisatie meer greep kan krijgen op systeemsoftware die in een produktie-omgeving is geïmplementeerd. Het beheersen hiervan is van essentieel belang omdat met software bedrijfsfuncties van een organisatie worden gerealiseerd en ondersteund. Deze functionaliteit dient niet ongewenst of onbedoeld veranderd te worden. Slechts na expliciete acceptatie en autorisatie door de eigenaar van de bedrijfsfuncties mogen deze aanpassingen in produktie worden gerealiseerd.

INLEIDING

De beheersing van de kwaliteit van de geïmplementeerde software in produktie is een belangrijk onderdeel van kwaliteit van geautomatiseerde informatieverwerking. Naast *betrouwbaarheid, vertrouwelijkheid* en *continuïteit* is het kwaliteitsaspect *integriteit* van belang, waarbij in de context van dit artikel onder *integriteit* wordt verstaan: de mate van overeenstemming tussen de feitelijk geïmplementeerde functionaliteit en de vooraf gedefinieerde en door de eigenaar geaccepteerde specificaties van software ([IBMD]). Een blijvende integriteit van systeemsoftware-componenten wordt zeer sterk bevorderd met adequate beheersprocedures. In de praktijk schort het vaak hieraan. In dit artikel worden de concepten voor adequate beheersprocedures besproken.

Voor het beheersen van *applicatiesoftware* is met de ITIL-'standaarden' een adequaat concept ontwikkeld, dat inmiddels uitgebreid in de literatuur is beschreven (o.a. [ITIL92] en [ITIL93]). Het concept is gebaseerd op scheiding tussen de test-, acceptatie- en produktie-omgeving met bijbehorende overdrachtsmechanismen. Dit concept blijkt voor applicatiesoftware in de praktijk goed te voldoen.
Voor systeemsoftware blijkt dit concept niet onverkort van toepassing te zijn. Onder *systeemsoftware* wordt verstaan de combinatie van software en parameters die benodigd zijn om de hardware en overige services aan te sturen. Hij omvat naast besturingssoftware (het operating-systeem) ook de uitbreidingen hierop zoals datacommunicatie- en transactieverwerkende software, software voor gegevensbenadering zoals database-managementsystemen, software ter beheersing van toegangscontrole, alsmede de software die nodig is voor het maken van wijzigingen van toepassingen zoals vertaalprogramma's ([Koed86]). Kenmerkend voor *systeemsoftware* zijn de vele parameters die moeten worden ingesteld. Deze instellingen worden vaak bewerkstelligd met 'run time'-commando's. Met de term 'run time' wordt bedoeld dat deze componenten rechtstreeks in de produktie-omgeving worden aangepast zonder dat een overdrachtstraject, met scheiding tussen ontwikkeling, acceptatie en distributie, wordt doorlopen. Het toepassen van een overdrachtsmechanisme voor het beheersen van deze parameters is in veel gevallen niet mogelijk.
Voor het beheersen van software is het van belang dat de eigenaar de wijzigingen autoriseert. In de praktijk blijkt dat voor systeemsoftware en de bijbehorende parameters en tabellen, kortweg aangeduid als *systeemsoftware-componenten*, in de organisatie vaak niet eenduidig een eigenaar is aangewezen.

Bovengenoemde aspecten worden uitgediept in de in dit artikel te behandelen concepten. Er zal worden aangegeven hoe het principe van functiescheiding een beheersingsconcept biedt voor systeemsoftware-componenten die 'run time' gewijzigd (moeten) worden. Gemakshalve zullen in dit artikel de termen systeemsoftware-component en parameter door elkaar worden gebruikt.

Scoor uw actuele organisatiestatus met betrekking tot de beheersing van uw produktie-omgeving!

Opdat de lezer kan bepalen in hoeverre dit artikel nuttig is voor het rekencentrum waarvoor men zijn/haar diensten verleent, is hieronder een aantal vragen opgesteld. Het puntentotaal geeft een indicatie voor de mate van beheersing van systeemsoftware-componenten in de produktie-omgeving van de organisatie.
Beantwoord de onderstaande zes vragen en tel de behaalde punten op.

• Kent uw rekencentrum zodanige procedures dat het aanbrengen van 'run time'-wijzigingen van systeemsoftware-parameters (zoals het wijzigen van de system-wide password-change-interval of het opnemen van een load-module in een APF-library) een autorisatietraject doorloopt?

- strikt formele autorisatie door eigenaren van parameters [1 punt]
- variëteit aan autorisatieprocedures [3 punten]
- informele autorisatie + incidentele controle achteraf [5 punten]

• Is de acceptatiefunctie ten behoeve van autorisatie van wijzigingen van softwarecomponenten ingevuld in uw organisatie?

- acceptatiefunctie geheel ingevuld [1 punt]
- project ter invulling van acceptatiefunctie is lopende [3 punten]
- niet ingevuld [5 punten]

• Kent uw organisatie een overdrachtstraject voor zowel applicatieve als systeemsoftware, die gebaseerd is op het magazijnprincipe?

- magazijnconcept zowel voor applicatiesoftware als systeemsoftware [1 punt]
- magazijnconcept wel voor applicatiesoftware maar nog niet voor systeemsoftware [3 punten]
- geen formeel overdrachtstraject [5 punten]

• Wordt in de verplicht op te leveren inrichtingsnota/implementatievoorstel voor systeemsoftware onderscheid gemaakt naar typen parameters ten behoeve van het te doorlopen autorisatietraject?

- parameters in inrichtingsnota worden naar typen onderscheiden [1 punt]
- slechts kritieke systeemsoftware-componenten worden beschreven [3 punten]
- systeemsoftware-parameters worden niet in inrichtingsnota beschreven [5 punten]

• Vinden er binnen uw organisatie periodieke rapportages plaats van wijzigingen van geïmplementeerde systeemsoftware?

- periodieke rapportage aan VTO-acceptant [1 punt]
- incidentele rapportages door afd. Interne Controle [3 punten]
- slechts rapportage van systeemlogging [5 punten]

• Wordt bij support-verlening gebruik gemaakt van een algemeen support-user-id of van persoonlijke user-ids met tijdelijk extra toegekende bevoegdheden?

- persoonlijke user-ids met tijdelijk extra support-bevoegdheden [1 punt]
- algemene support-id die slechts wordt toegekend na expliciete autorisatie [3 punten]
- algemene support-user-id [5 punten]

Uitslag

6 – 10 punten: Uw organisatie kent formele beheersingsconcepten. Het artikel geeft u een theoretisch kader omtrent uw geïmplementeerde beheersingsconcepten voor systeemsoftware.

11 – 20 punten: In uw organisatie zijn beheersingsconcepten in wording. Het artikel helpt u bij het implementeren van sluitende beheersingsconcepten voor systeemsoftware.

21 – 30 punten: In uw organisatie zijn weinig formele beheersingsconcepten toegepast. Het artikel verschaft u inzichten omtrent beheersingsconcepten voor systeemsoftware en moedigt implementatie ervan aan.

Volledige beheersing tot in alle details van de systeemsoftware in produktie is slechts theoretisch mogelijk. De ontvouwde concepten zijn dan ook bedoeld om het management van een verwerkingsorganisatie handvatten aan te reiken om het kwaliteitsaspect *integriteit* van de geautomatiseerde informatieverwerking op een voor de betreffende organisatie aanvaardbaar niveau te brengen en te houden.

Belang van het beheersen van systeemsoftware

Kenmerkend voor de operationele omgeving is het resultaatgericht werken van de informatiesystemen. De veel gehoorde kreet 'de produktie gaat voor' houdt veelal in dat autorisatie-aspecten op de achtergrond raken indien hiervoor geen expliciete beheersprocedures zijn ontwikkeld die door het management worden gedragen. Systeemparameters kunnen diverse vormen aannemen en op diverse plaatsen in de systemen aanwezig zijn. Zo zijn bijvoorbeeld binnen een schedule-pakket de in de database opgeslagen kalenderdagen als functionele parameters te zien. Een goed produktieresultaat komt onmiddellijk in gevaar op het moment dat niet de nodige zorgvuldigheid wordt betracht bij het instellen van deze parameters op het systeem. Beheersprocedures dienen zorg te dragen voor een blijvende correcte instelling van de parameters. Een ander voorbeeld zijn de parameters van een beveiligingspakket die 'run time' worden ingesteld. De waarde van de 'user-id revoke-period' bepaalt de tijdsduur in dagen, waarna de geldigheid van de user-id automatisch door het systeem wordt ingetrokken ('revoked') indien in de tussentijd niet met de user-id is aangelogd. Wijzi-

ging van deze parameter kan de beveiliging van het systeem in sterke mate beïnvloeden.
Een derde voorbeeld zijn de tabellen binnen het beveiligingspakket RACF die de functionaliteit bepalen. Deze tabellen worden 'run time' gewijzigd. Voorbeelden hiervan zijn het opnemen van een EXIT in de produktionele RACF, waarmee de autorisatie door RACF omzeild kan worden, en het opnemen van een programma in de Program Properties Table, waarmee de password-beveiliging omzeild kan worden. Het beheersen van deze 'run time'-wijzigingen is van belang voor een effectieve werking van de beveiliging.
Deze voorbeelden illustreren de waarde van het belang van het beheersen van systeemparameters.

Een organisatie loopt de volgende risico's als software zonder adequate beheersprocedures in produktie draait ([SAC91]):

- Niet volledig geteste software kan processen doen vastlopen en ongewenste vertraging van de produktie veroorzaken of kan processen op onjuiste wijze laten verlopen zodat onjuiste uitkomsten worden verkregen.

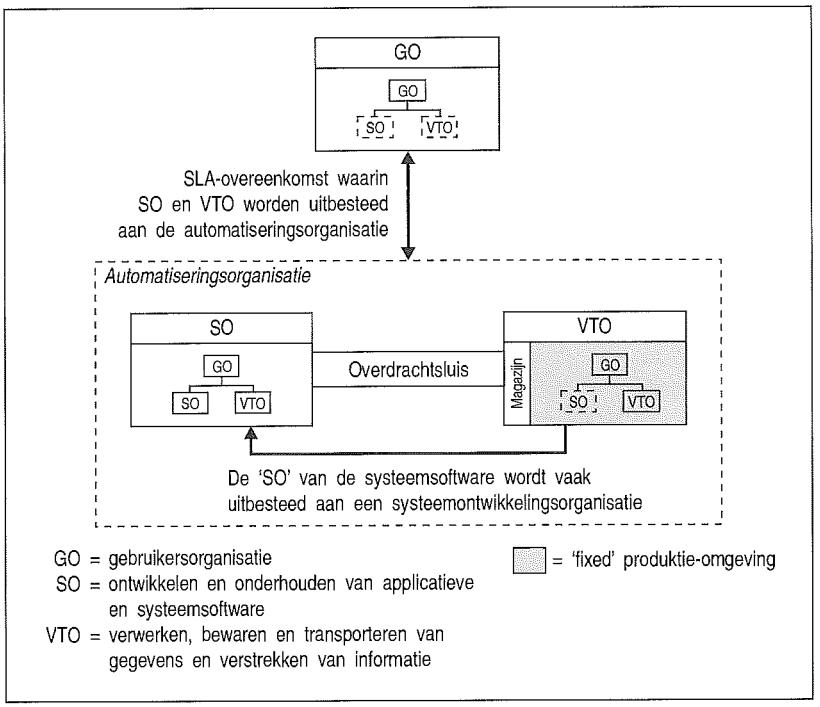
- Ongeautoriseerde veranderingen in de parameters kunnen wellicht de acute problemen in de onderhavige processen oplossen maar andere problemen, ook op de langere termijn, veroorzaken.

- Ongeautoriseerde veranderingen in de software kunnen de integriteit van bedrijfsgegevens of van het bedrijfsproces aantasten of kunnen gebruikt worden om fraude mee te plegen.

Als illustratie van de diverse beheersingsconcepten worden in het vervolg van dit artikel voornamelijk voorbeelden gegeven uit één van de gebieden van systeemsoftware, namelijk parameters van het beveiligingspakket RACF. Voor de parameters van overige systeemsoftware kunnen de beheersingsconcepten op een analoge wijze worden toegepast.

DRIE FUNCTIONELE ORGANISATIES

Naast de gebruikersorganisatie (GO) zijn met de automatisering twee additionele organisaties ontstaan: de organisatie van de systeemontwikkeling en systeemonderhoud (SO) en de organisatie om de gegevens te verwerken en de datacommunicatie (transport) te verzorgen (VTO).
Het automatiseren van bedrijfsprocessen binnen de GO houdt in feite in dat activiteiten worden uitbesteed aan de SO en aan de VTO (zie figuur 1). Bij uitbesteding is er sprake van opdrachtverstrekking aan derden, waarbij ervan wordt uitgegaan dat die derde zorgt voor kwalitatief goed werk. De definitie van kwaliteit in dezen wordt vastgelegd in een Service Level Agreement (SLA), ook wel genoemd: Automatiserings Kwaliteit Overeenkomst. Onderwerpen van een SLA zijn onder andere: minimaal gegarandeerde beschikbaarheid van het systeem, responstijden, backup-frequentie, uitwijkprocedures, en helpdesk-functionaliteiten ([ITIL90b]).



Figuur 1. De drie functionele organisaties.

Het uitbesteden van de bedrijfsprocessen van de GO aan de VTO, zoals vastgelegd in een SLA, houdt in dat de GO ervan uit mag gaan dat de VTO zelf zorg draagt voor de betrouwbaarheid en continuïteit van de verwerking binnen de VTO en dat de GO deze niet steeds zelf hoeft vast te stellen. Dit *SLA-concept*, dat Kocks het STOP-concept noemt ([Kock93]), houdt ook in dat de gebruiker mag aannemen dat de programmatuur inderdaad werkt zoals deze door de ontwikkelorganisatie is gebouwd en door de gebruiker is geaccepteerd. Bij het SLA-concept dient de automatiseringsorganisatie derhalve zelf zorg te dragen voor adequate beheersmaatregelen als functiescheiding en overdrachtsmechanismen.

In figuur 1 komt tevens een beheersingsconcept tot uitdrukking waarmee de VTO aan de GO garandeert dat er slechts wordt gewerkt met programmatuur zoals deze door de gebruiker (eigenaar) is geaccepteerd: functiescheiding tussen ontwikkeling (SO), acceptatie (GO) en verwerking (VTO) en een overdrachtsmechanisme voor de ontwikkelde en geaccepteerde software.

Functiescheiding in een software-omgeving

Ten behoeve van beheersing van wijzigingen van software (zowel applicatiesoftware als systeemsoftware) kunnen de volgende functies worden onderscheiden:
- *registreren:* het 'vertalen' van functionele wensen naar een softwarematige beschrijving en deze vastleggen in een inrichtingsvoorstel of wijzigingsaanvraag. De registrerende functie bestaat dus niet zozeer uit het formeel invullen van een wijzigingsaanvraag als wel uit het op de juiste wijze 'vertalen' van een door de GO gewenste functionaliteit naar een softwareinrichting;

- *beschikken:* het autoriseren en daarmee accepteren van de (gewijzigde) software-inrichting;
- *uitvoeren:* het daadwerkelijk aanbrengen van de wijzigingen in de produktie-omgeving;
- *bewaren:* het bewaken van de in produktie genomen software, inclusief de inhoud van de functieverdeelstaat;
- *controleren:* het controleren dat wijzigingen slechts worden uitgevoerd volgens een daartoe vastgelegde procedure, gebaseerd op functiescheiding en het toetsen van implementatie aan de normen.

Bij het SLA-concept dient de automatiseringsorganisatie zelf zorg te dragen voor adequate beheersmaatregelen als functiescheiding en overdrachtsmechanismen.

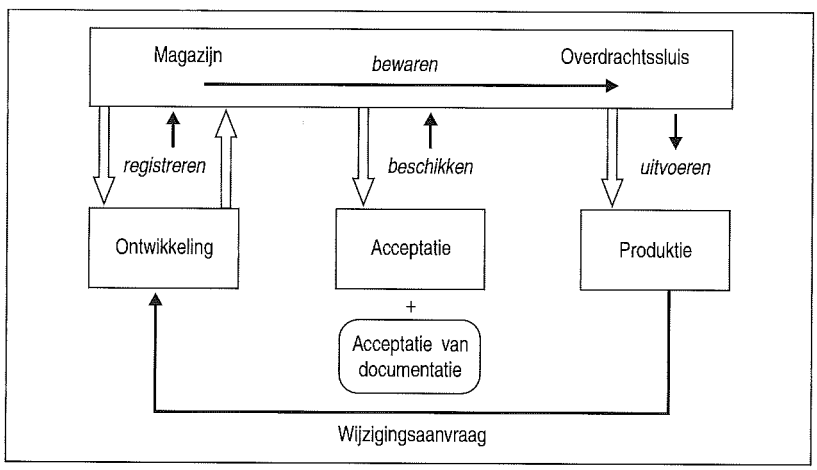
De bewarende functie wordt vervuld door het magazijn. Hier wordt het versiebeheer gedaan van alle software. De controlerende functie kan op meerdere manieren worden vervuld, onder andere door de afdeling Interne Controle. In dit artikel wordt op deze functie, evenals op de bewarende functie, slechts zijdelings ingegaan.

De functiescheiding tussen het registreren, beschikken en uitvoeren leidt in een automatiseringsomgeving primair tot scheiding tussen ontwikkeling, acceptatie en produktie:

- De ontwikkelfunctie is verantwoordelijk voor de ontwikkeling, de functionele parametrisering en de ondersteuning (support) van het softwaregebruik. De ontwikkelafdeling mag niet in de produktie-omgeving actief zijn, tenzij via specifieke procedures om support te verlenen.

- De acceptatiefunctie mag slechts programmatuur accepteren en distribueren die door de ontwikkelafdeling is aangeleverd en de acceptatieafdeling mag hierin geen wijzigingen aanbrengen. (N.B.: Uit pragmatische overwegingen verricht de acceptatie-afdeling voor een aantal parameters tevens de uitvoering van de wijzigingen; met berichtgeving aan de produktie-afdeling.)

- De produktie-afdeling mag slechts programmatuur gebruiken die formeel is geaccepteerd en mag hierin geen wijzigingen aanbrengen (behoudens operationeel gerichte parameters).



Figuur 2. Functiescheiding met behulp van het magazijnprincipe ([Broe93]).

In figuur 2 is het overdrachtsmechanisme in beeld gebracht. Hierbij staat het *magazijn* centraal. In het magazijn dient de software, nadat de ontwikkelingsfase is afgerond, veilig opgeslagen te worden, waarna een kopie van de software vanuit dit magazijn beschikbaar wordt gesteld voor acceptatie. Na een succesvolle acceptatie kan de originele software worden gedistribueerd en in produktie worden genomen.

In het magazijn dienen de aanwezigheid (voorraad) en de bewegingen (opname, status, distributie, etc.) van de software te worden geregistreerd. Iedere wijziging van softwarecomponenten in de produktie-omgeving dient in beginsel plaats te vinden in de ontwikkelomgeving vanwaar de gewijzigde software aan het magazijn wordt aangeboden ter acceptatie en distributie. Deze gang van zaken wordt *change management* genoemd.
Er moet worden gewaarborgd dat de software in het magazijn en in produktie niet gewijzigd kan worden. Het magazijn dient daartoe onderdeel te zijn van de beveiligde omgeving.
Een nieuwe software-release van het beveiligingspakket RACF, aangeleverd door de leverancier, wordt bijvoorbeeld in de ontwikkelomgeving getest en eventueel op de wensen van de organisatie toegesneden ('customized'). Vervolgens wordt deze software doorgesluisd naar de acceptatieomgeving, waar acceptatie door de VTO-organisatie van de release zal plaatsvinden alvorens deze naar de produktie-omgeving wordt gedistribueerd.

Er zijn inmiddels verschillende softwarefabrikanten die produkten op de markt hebben gebracht waarmee het change management van softwarereleases goed beheersbaar is. Deze produkten zijn gebaseerd op het magazijnprincipe met afgedwongen scheidingen tussen ontwikkeling, acceptatie en distributie. Voorbeelden hiervan zijn INFOMAN (IBM), ENDEVOR (LEGENT) en PANVALET/PANAPT.

Om technische redenen is het vaak niet mogelijk of wegens voortgang van de produktie ongewenst om alle wijzigingen van systeemsoftware-componenten in de produktie-omgeving via het overdrachtstraject te laten lopen. De parameters zullen dan 'run time' moeten worden gewijzigd. In dit geval is het beheersingsconcept dat is gebaseerd op het overdrachtsmechanisme waarmee functiescheiding softwarematig wordt afgedwongen, niet toepasbaar. Een voorbeeld hiervan is het toekennen van de RACF-bevoegdheid SPECIAL aan een user-id. Deze bevoegdheid wordt met een commando in de produktie-omgeving toegekend aan een user-id.
Bij het aanbrengen van 'run time'-wijzigingen is testen en acceptatie niet mogelijk en dient functiescheiding tussen registratie, autorisatie en uitvoering procedureel te worden afgedwongen. Er moeten procedures worden ontwikkeld en gevolgd die

ervoor zorgen dat de wijzigingen eerst door de eigenaar geautoriseerd worden alvorens deze 'run time' in de produktie-omgeving worden aangebracht. Alvorens nader in te gaan op deze procedures voor functiescheiding zal eerst het eigenaarschap van software, en in het bijzonder van systeemsoftware, worden behandeld.

EIGENAARSCHAP VAN SOFTWARE

Het vaststellen van eigenaarschap van software is van belang om softwarewijzigingen door de juiste personen te kunnen laten autoriseren. Voor data, voor applicaties en voor systeemsoftware zijn verschillende eigenaren aan te wijzen.

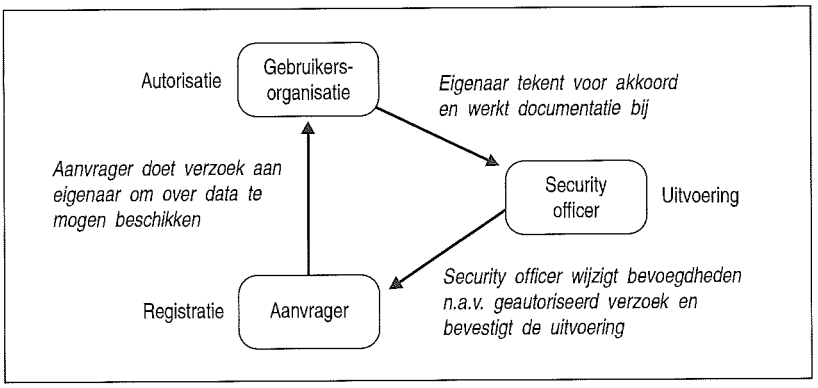
Eigenaarschap van data

Voor *data* is de eigenaar te vinden binnen de gebruikersorganisatie. Een wijziging bijvoorbeeld in een rentetabel dient te worden geautoriseerd door de eigenaar van deze tabel, de afdeling Rentestaffeling. Ook zal een wijziging van de toegangsmatrix van de tabel slechts mogen worden aangebracht na autorisatie door de eigenaar van de data. De toegangsmatrix kan een onderdeel zijn van de applicatie, maar de beveiliging van de tabel kan ook zijn ingericht met behulp van een beveiligingspakket (bijvoorbeeld RACF) dat beheerd wordt door een security officer binnen de GO of een Security Desk binnen de VTO.

In figuur 3 wordt de functiescheiding ten behoeve van wijzigingen van toegangsregels voor data weergegeven.

Eigenaarschap van applicatiesoftware

Ook *applicaties* worden gebouwd voor een gebruikersorganisatie en zijn derhalve eigendom van de afdeling die hiervoor functioneel verantwoordelijk is. Zo zal het eigenaarschap van het personeelsadministratiesysteem liggen bij de afdeling Personeelszaken. Deze afdeling dient aanvragen tot wijzigingen van functionaliteit (bijvoorbeeld nieuwe releases, wijzigingen in de functieverdeelstaat of in de toegangsmatrix) te accepteren en te autoriseren. Indien de VTO de tabellen van de toegangsregels beheert (bijvoorbeeld door een Security Desk), dient de Security Desk de wijzigingsaanvraag slechts te honoreren als deze voorzien is van een handtekening van de gebruikersafdeling. De leiding van de gebruikersafdeling delegeert de beschikkende functie vaak aan een functionaris die ook de acceptatietaak vervult bij implementatie van deze applicatiesoftware. Deze taak kan belegd zijn bij een Business System Manager (BSM) of bij een afdeling Informatiemanagement (IM). Beide laatstgenoemde zijn onderdeel van de gebruikersorganisatie en voeren hun beschikkende functie namens deze uit.



Figuur 3. Functiescheiding bij wijziging van toegang tot data.

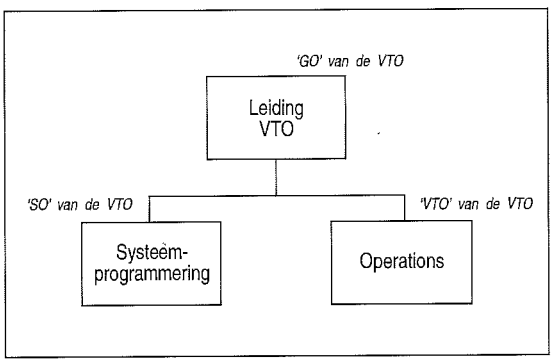
Eigenaarschap van systeemsoftware

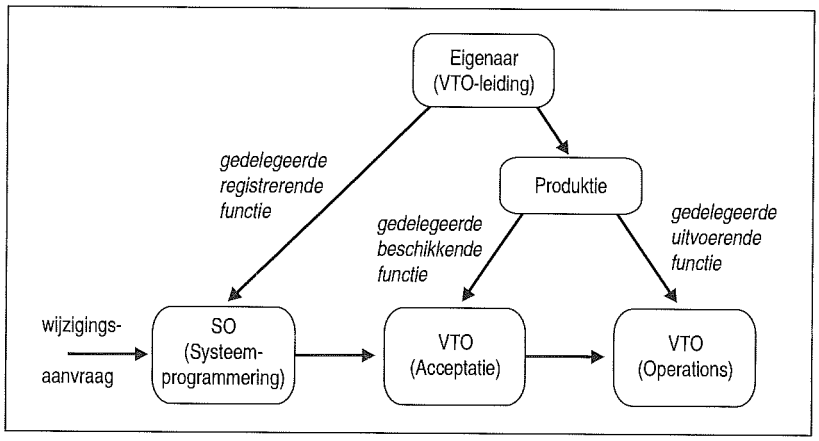
Systeemsoftware wordt niet expliciet ontwikkeld voor een (eind)gebruikersorganisatie. Wel worden hieraan eisen gesteld die voortvloeien uit de SLA-overeenkomst tussen de VTO en de GO.
De systeemsoftware maakt deel uit van de infrastructurele voorzieningen die de VTO nodig heeft om haar taken te kunnen verrichten. De functionele eisen voor deze voorzieningen zullen derhalve door de leiding van de VTO gesteld worden. De leiding van de VTO (de 'GO' van de VTO; zie figuur 4) is dan ook eigenaar van de infrastructuur waarop de verwerking en het transport van de gegevens plaatsvinden en dus ook van de systeemsoftware (en de bijbehorende parameters) die deel uitmaakt van de infrastructuur. De eisen die de 'GO' van de VTO aan de functionaliteit van systeemsoftware stelt, zijn input voor de 'SO'-afdeling die de systeemsoftware dient te ontwikkelen c.q. aan te schaffen.

De 'SO' van de VTO (de afdeling Systeemprogrammering) heeft met het opstellen van het inrichtingsvoorstel of de wijzigingsaanvraag een *registrerende* functie. In de praktijk blijkt dat de afdeling Systeemprogrammering vaak buiten de eigenlijke VTO-organisatie wordt belegd om voldoende afstand tot de produktie-omgeving te waarborgen.

De 'VTO' van de VTO (ofwel de afdeling Operations) mag vanwege de eisen van integriteit niet zelfstandig wijzigen in produktie, maar heeft slechts een *uitvoerende* taak van geautoriseerde wij-

Figuur 4. Organogram van een VTO-organisatie.





Figuur 5. Delegatie van functies.

zigingen. Voor Operations is de produktie-omgeving een vaste, niet wijzigende ('fixed') omgeving.

De 'GO' van de VTO zal de *beschikkende* functie delegeren aan de afdeling die de acceptatie van systeemsoftware doet. De accepterende afdeling dient inhoudelijk te beoordelen of de aangeleverde wijziging in de software daadwerkelijk overeenkomt met de beschreven functionaliteitswijziging. Vanwege de complexiteit van systeemsoftware vereist dit een hoge mate van deskundigheid, die bij de 'VTO' van de VTO niet standaard aanwezig is omdat de organisatie deze specifieke deskundigheid nu juist heeft belegd bij de ontwikkelafdeling Systeemprogrammering. Vaak zal de acceptatie van systeemsoftware door de VTO dan ook gebeuren in samenwerking met deze ontwikkelafdeling. Hierdoor treedt functievermenging op tussen de beschikkende functie (acceptant) en de registrerende functie (ontwikkelaar). Dit zou kunnen inhouden dat een andere functionaliteit wordt ingevoerd dan gewenst door de eigenaar (GO). Desgewenst kan in afzonderlijke gevallen, bijvoorbeeld ten behoeve van eenmalige acceptatie van kritieke of complexe systeemsoftware-releases, een beroep worden gedaan op de deskundigheid van de EDP-auditor ter ondersteuning en waarborging van een onafhankelijke beschikkende functie ([NGI89]).

Om de verantwoordelijkheid voor de systeemsoftware-parameters naar de produktie-omgeving te kunnen overdragen zijn deze parameters vastgelegd in een *inrichtingsnota*[1], ook wel implementatievoorstel genoemd. Deze inrichtingsnota dient bij de overdracht van de ontwikkelde software mede ter acceptatie te worden opgeleverd.

In figuur 5 wordt het delegeren van de diverse functies uitgebeeld.

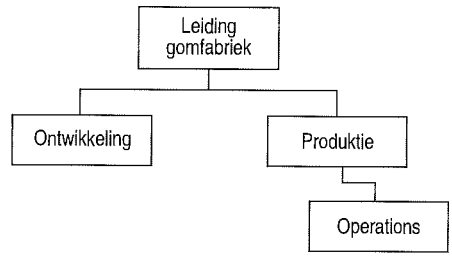
'Delegatie van functies' in een gomfabriek

In een chemische fabriek wordt gom geproduceerd. De grondstoffen van de gom dienen tijdens het fabricageproces op een bepaalde – ideale – temperatuur te worden gehouden. Bij een andere dan de 'ideale' temperatuur treedt verlies aan kwaliteit van de geproduceerde gom op. De produktiemedewerker kan de temperatuur instellen. Als na een aantal werkuren blijkt dat een bepaalde produktie'batch' langer gaat duren dan de werktijd van de produktiemedewerker, bestaat de (niet ondenkbeeldige) neiging van de produktiemedewerker om de temperatuur enigszins op te voeren zodat het fabricageproces sneller verloopt en hij op tijd naar huis kan.

In deze casus is de temperatuurregeling te vergelijken met 'systeemsoftware' en de oven is te vergelijken met de 'hardware' waarop het produktieproces draait. De temperatuurstand is een functionele parameter van de 'systeemsoftware'.
Geconcludeerd kan worden dat de kwaliteit van het eindprodukt mede bepaald wordt door de juiste instellingen van 'systeemsoftware'-parameters.

De beheersvraag van het management van de gomfabriek betreft onder andere het onder controle hebben van het juist instellen van de temperatuur door de produktiemedewerkers. De leiding zal het uitvoeren van het produktieproces en de samenhangende parameters delegeren aan een afdeling (Operations), die hiervoor de expliciete verantwoordelijkheid krijgt. Deze afdeling dient het fabricageproces te verrichten met de normatieve temperatuurinstelling zoals deze door de afdeling Ontwikkeling is aangegeven.

Wijziging van de normatieve temperatuur, die bij een bepaald fabricageproces hoort, mag slechts worden



aangebracht nadat de 'eigenaar' van het fabricageproces toestemming heeft gegeven.

Om deze wijzigingen te beheersen heeft de eigenaar functiescheiding toegepast.
Tijdens de ontwikkelingsfase van het gehele fabricageproces is het vaststellen van de optimale temperatuur (de 'registrerende' functie) voor dit proces een taak van de afdeling Ontwikkeling.
De afdeling Produktie accepteert en implementeert namens de leiding van de gomfabriek het produktieproces, zoals dat is opgeleverd door de afdeling Ontwikkeling.
Het management van de afdeling Produktie zal de uitvoering van het produktieproces delegeren aan de produktiechef met zijn produktiemedewerkers (afdeling Operations).

Als er een (functionele) verandering gewenst wordt en deze functionele wens vertaald dient te worden in fabricageparameters (registrerende functie), mag de afdeling Produktie deze verandering niet eigenhandig doorvoeren. De 'registrerende' functie is immers belegd bij de afdeling Ontwikkeling, die de technische know-how heeft om alle consequenties terdege te doordenken alvorens de verandering aan de afdeling Produktie aan te bieden.

1. De inrichtingsnota beschrijft de softwarematige inrichting met alle functionele en operationele parameters en de bijbehorende instellingen. Per parameter is een verantwoordelijke acceptant omschreven. Tevens is een security matrix *opgenomen in de inrichtingsnota. Met de security matrix wordt het overzicht bedoeld dat de autorisaties beschrijft van de gebruikers van de diverse systeemsoftwarecomponenten.*

DELEGATIE VAN FUNCTIES

Wijzigingen van systeemsoftware dienen geautoriseerd te worden door de eigenaar. De eigenaar delegeert deze autorisatiefunctie naar de afdeling die de acceptatie van de software doet.
Met het begrip gedelegeerde functie wordt aangegeven dat iemand optreedt namens iemand anders en ook slechts voor een afgebakend terrein. Dit afgebakende terrein is vastgelegd in de inrichtingsnota en de bijbehorende beveiligingsparagraaf, die met de software door de SO is overgedragen aan de VTO.
Om te weten tot hoe ver het mandaat van de acceptant reikt voor autorisatie van softwarewijzigingen zonder de registrerende functie te hoeven raadplegen, dient een onderscheid te worden gemaakt in omvang van de wijziging. Hierbij dient tevens een onderscheid te worden gemaakt tussen parameters die de functionaliteit bepalen of beïnvloeden (*functionele parameters)* en parameters die aanpassing behoeven als gevolg van operationele vereisten (*operationele parameters*).

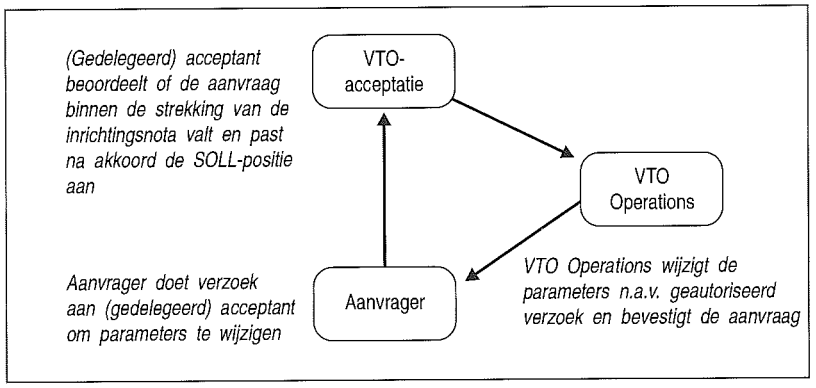
Operationele parameters

Onder operationele parameters worden die componenten verstaan die vanwege operationele behoeften worden gewijzigd. Dit betreffen dus geen functionele wijzigingen maar exploitatiegerichte wijzigingen die de afdeling Operations dan ook zonder verdere autorisatie mag aanbrengen; dit behoort immers tot de taakstelling van deze afdeling. Voorbeelden hiervan zijn: het aanpassen van storage-classes en van output-verzamelparameters.

Functionele parameters

De functionele parameters zullen na implementatie in de produktie-omgeving vanuit de operationele invalshoek gezien geen verdere wijzigingen ondergaan.
Deze componenten, waaronder ook parameters die 'run time' worden gewijzigd, behoren voor de afdeling Operations dus tot de 'fixed' produktieomgeving. De functionele systeemsoftware en parameters mogen immers pas worden gewijzigd nadat hiervoor vanuit de gebruikerszijde een 'functioneel verzoek' is ingediend. Met 'functioneel verzoek' wordt hier bedoeld dat het gaat om een wijziging en/of uitbreiding van de functionaliteit van de software. Dit kan het verzoek zijn voor een geheel nieuwe release maar ook het aanvragen van aanvullende toegangsbevoegdheden voor reeds geïmplementeerde systeemsoftware.
Aangezien de 'vertaling' van een 'functioneel verzoek' naar softwarematige inrichtingen is gedelegeerd aan de SO zullen de wijzigingen van functionele parameters worden geregistreerd door de afdeling Systeemprogrammering.

Ten behoeve van autorisaties van wijzigingen van functionele parameters dient een onderscheid te worden gemaakt in:

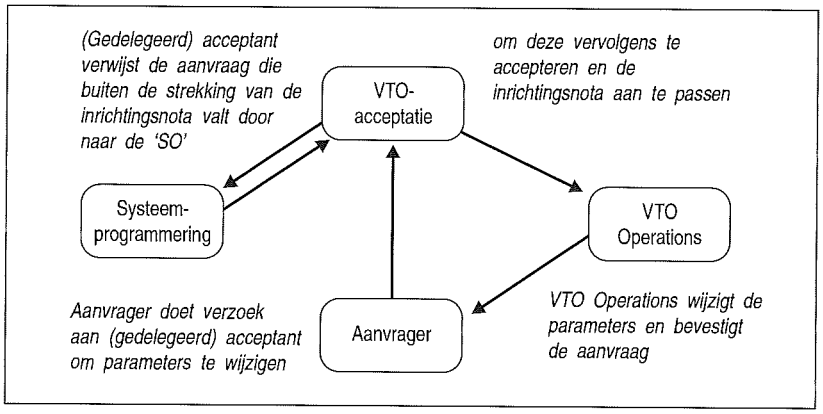


Figuur 6. Functiescheiding bij wijzigingen van functionele parameters van systeemsoftware, die binnen de strekking van de inrichtingsnota vallen.

a. wijzigingen die binnen de strekking van de inrichtingsnota vallen;
b. wijzigingen die de strekking van de inrichtingsnota overstijgen.

Ad a. Wijzigingen die binnen de strekking van de inrichtingsnota vallen
Wijzigingen van parameters die binnen de strekking van de inrichtingsnota vallen en dus binnen de beschreven functionaliteit blijven, kunnen rechtstreeks worden geautoriseerd door de acceptant; immers dit valt binnen het mandaat van de aan hem gedelegeerde beschikkende functie. Een voorbeeld hiervan is het toevoegen van een datum in een schedule-pakket, dat rechtstreeks kan worden geautoriseerd door de VTO-acceptant van deze software en niet vooraf hoeft te worden geregistreerd door de afdeling Systeemprogrammering. Deze functionaliteit is immers reeds in de inrichtingsnota beschreven.

Ad b. Wijzigingen die verder reiken dan de strekking van de inrichtingsnota
Wijzigingen van componenten die verder reiken dan de strekking van de inrichtingsnota en dus nog niet zijn geregistreerd, mogen slechts worden geaccepteerd en opgebracht nadat de registratie heeft plaatsgevonden. De eigenaar heeft deze functie belegd bij de afdeling Ontwikkeling en deze zal derhalve moeten worden betrokken in het changetraject. Soms wordt de afdeling Ontwikkeling 'functioneel eigenaar' genoemd. Beter is te spreken van *functioneel beheerder*; zij beheert namelijk de juiste vertaling van functionaliteitseisen naar software-inrichting.
Voorbeelden van deze functionele systeemsoftware-componenten zijn:
- de 'harde' software van het operating-systeem;
- de 'harde' software van een toegangsbeveiligingspakket;
- de 'harde' software van een databasemanagement-pakket;
- de inrichtingsparameters ervan, zoals configuratie-files van jobs;
- eenmalig in te stellen systeem-brede parameters van het operating-systeem (SYS1.PARMLIB van het MVS-operating-systeem);
- eenmalig in te stellen system-wide parameters van een toegangsbeveiligingspakket (password-change-interval en andere SETROPTS-waarden, entries van de PPT-tabel; SMF-exits binnen RACF).



Figuur 7. Functiescheiding bij wijzigingen van functionele parameters van systeemsoftware, die buiten de strekking van de inrichtingsnota vallen.

Bij invoering van systeemsoftware dient de implementatie in een inrichtingsnota te zijn beschreven. De acceptant dient namens de eigenaar deze documentatie op juistheid en volledigheid te controleren alvorens de 'change' (wijzigingen én documentatie!) te accepteren.

De VTO-acceptatiefunctie mag volgens het principe van functiescheiding geen wijzigingen buiten de strekking van de inrichtingsnota autoriseren.

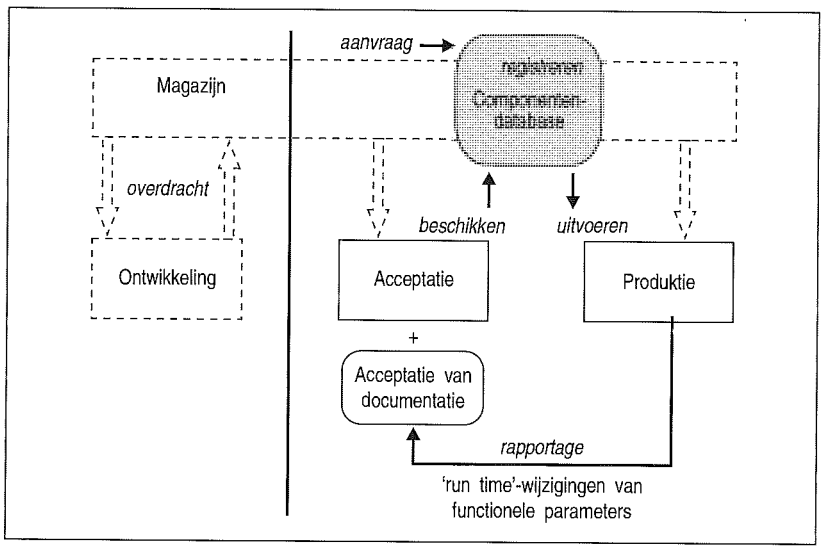
Het delegeren van de beschikkende functie houdt in dat autorisaties van wijzigingen periodiek moeten worden gerapporteerd aan de uiteindelijke eigenaar opdat deze kan vaststellen of er buiten het mandaat om autorisaties zijn verstrekt. Hier ligt een taak voor de afdeling Interne Controle, die de controlerende functie namens de eigenaar uitvoert.

PROCEDURELE FUNCTIESCHEIDING

Autorisatie vooraf van reguliere 'run time'-wijzigingen

Figuur 8. Functiescheiding bij 'run time'-wijzigingen van functionele systeemsoftware.

Kenmerkend voor wijzigingen van systeemsoftware is de 'run time'-wijze waarop deze in de produktie-omgeving worden aangebracht. Hierbij is het magazijnconcept niet van toepassing en moet worden gesteund op procedurele functiescheiding.



De procedurele functiescheiding kan worden ondersteund door het gebruik van een database waarin alle systeemsoftware-componenten beschreven staan en waarin de waarden en instellingen van en de toegangsrechten tot alle componenten zijn vastgelegd (SOLL-positie). In feite is dit een geautomatiseerde vastlegging van de inrichtingsnota, inclusief de security-matrix voor systeemsoftware-componenten (zie figuur 8).
Procedureel, en indien mogelijk softwarematig, moet zijn afgedwongen dat deze componenten slechts in de produktie-omgeving kunnen worden gewijzigd nadat de wijzigingen eerst in deze componentendatabase geautoriseerd zijn. Het Britse overheidsorgaan CCTA spreekt over een geïntegreerde configuratiedatabase ([ITIL90b]). Deze werkwijze houdt in dat van iedere softwarecomponent de normatieve waarde in deze database moet zijn ingevuld. Voor een juiste autorisatie dient ook de specifieke acceptant per component vermeld te zijn, zodat softwarematig getoetst kan worden of de juiste acceptant heeft geautoriseerd met behulp van zijn user-id of een digitale handtekening. Ook kunnen in deze database de onderlinge relaties worden vastgelegd tussen systeemsoftware-componenten. Als de waarde van de ene component 'run time' wordt gewijzigd dan kan de databaseprogrammatuur afdwingen dat ook een andere gerelateerde component ('run time') wordt aangepast alvorens de wijziging kan worden geautoriseerd.
Om niet alle componenten in deze database op te hoeven nemen en te hoeven onderhouden, kan een organisatie ervoor kiezen om het gebruik van de componentendatabase-procedure slechts verplicht te stellen voor *kritieke* systeemsoftware-componenten, zodat alleen voor wijzigingen van deze componenten autorisatie *vooraf* gedwongen plaatsvindt.

Met het concept van de configuratiedatabase heeft de organisatie een instrument in handen om tot beheersing van de integriteit van softwarewijzigingen te komen: door het exclusief en gedwongen gebruik van de computer om de functies registratie, acceptatie en uitvoering uit te voeren, wordt functiescheiding door een volkomen automatisme gewaarborgd. Een voorwaarde voor het gebruik van dit beheersinstrument is dat de te beheersen (kritieke) systeemsoftware-componenten kunnen worden geïnventariseerd en in de produktie-omgeving afzonderlijk kunnen worden gewijzigd..

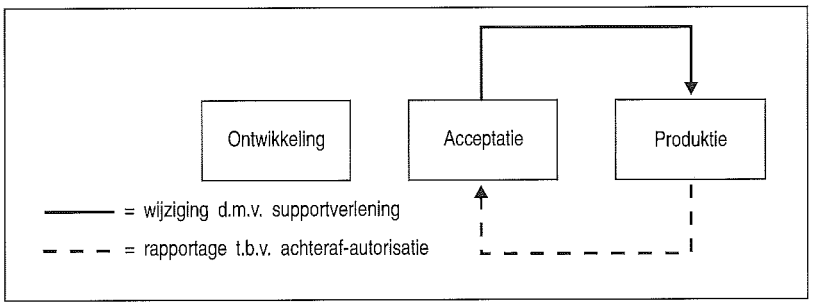
Autorisatie achteraf bij noodhulpverlening

Ook bij ondersteuning (support) bij het verhelpen van incidenten worden systeemsoftware-componenten 'run time' gewijzigd. Autorisatie *vooraf* van deze ingrepen is niet mogelijk. Bij support immers heeft de organisatie te maken met noodsituaties en moet er snel worden ingegrepen. Er dient dus een ander beheersingsconcept te worden gehanteerd dan bij het aanbrengen van reguliere 'run time'-wijzigingen.

Nulde-, eerste- en tweedelijnssupport
Men onderscheidt drie gradaties van support. Dit onderscheid heeft te maken met de mate waarin wijzigingen op produktie zijn aan te brengen met behulp van deze supportgereedschappen. Bij nuldelijnssupport gaat het veelal om het operationeel herstellen van het produktieproces door de operators zelf. Er is sprake van eerstelijnssupport indien het produktieproces hersteld moet worden met gereedschappen waarmee wijzigingen kunnen worden aangebracht die binnen de strekking van de inrichtingsnota vallen.
Met tweedelijnssupport wordt het herstellen van het produktieproces bedoeld dat noodzakelijk is als gevolg van fouten in het ontwerp of in de opzet van de software. Met deze gereedschappen kan de functionaliteit worden gewijzigd en kunnen dus wijzigingen worden aangebracht die buiten de strekking van de inrichtingsnota vallen.

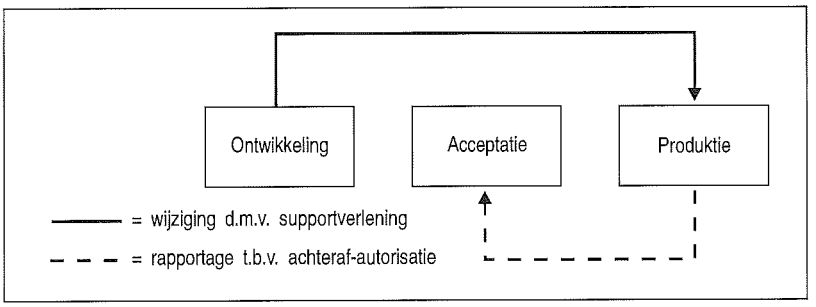
Dit onderscheid heeft gevolgen voor de te hanteren beheersingsconcepten in supportsituaties.
Om de integriteit van de geïmplementeerde software te waarborgen staan slechts de nuldelijnssupport-tools zonder verdere autorisatiebeperkingen ter beschikking aan de operators. Dit zijn slechts de tools waarmee het produktieproces kan worden geobserveerd of geanalyseerd. Op grond van deze waarnemingen kan de operator binnen zijn bevoegdheden zelf ingrijpen door bijvoorbeeld het proces opnieuw op te starten of een operationele parameter te wijzigen, of kan de operator door middel van een eerste analyse doelgerichte support inroepen.
De eerstelijnssupport wordt verricht door de afdeling binnen de VTO-organisatie die de acceptatiefunctie en het beheer van de systeemsoftware doet. Met deze eerstelijnssupport mogen slechts wijzigingen op de produktie-omgeving worden aangebracht die binnen de strekking van de inrichtingsnota vallen.
Indien wijzigingen noodzakelijk zijn die uitstijgen boven de strekking van de inrichtingsnota dient de hulp van de tweedelijnssupporter te worden ingeroepen.

Autorisatie achteraf door de acceptant op basis van rapportage
In het kader van het beheersen van wijzigingen op de produktie-omgeving dient de acceptant expliciet toestemming te verlenen voor de verrichtingen van de eerste- en tweedelijnssupport.[2] Vanwege het veelal spoedeisende karakter of het fysiek niet aanwezig zijn van de acceptant, zoals bij het 's nachts verlenen van support, zal de toestemming pas achteraf kunnen worden verkregen. Hiertoe dient het autorisatietraject aan de hand van rapportages van deze wijzigingen alsnog te worden doorlopen, waarbij wederom een onderscheid moet worden gemaakt tussen een wijziging die binnen de strekking van de inrichtingsnota valt en een wijziging die de strekking overstijgt.
Wijzigingen die binnen de strekking van de inrichtingsnota vallen, hoeven niet alsnog te worden geregistreerd door de SO. Wel dienen deze wijzigingen alsnog te worden geautoriseerd door de acceptant (VTO). De rapportages van deze wijzigingen dienen dan ook naar deze acceptant te gaan.



Wijzigingen die buiten de strekking van de inrichtingsnota vallen, dienen te worden geregistreerd door de afdeling Ontwikkeling, die verantwoordelijk is voor een juiste registratie van functionele wijzigingen. Vervolgens dient de wijziging alsnog het test- en acceptatietraject te doorlopen, waarbij de inrichtingsnota moet worden bijgewerkt. De rapportages van de wijzigingen dienen naar de afdeling Acceptatie te worden gestuurd.

Figuur 9. Autorisatie achteraf na support-verlening van wijzigingen van parameters die binnen *de strekking van de inrichtingsnota vallen.*



De acceptant (VTO) zal zijn geïnteresseerd in periodieke evaluatierapportages van het gebruik van de support-tools of in aantallen malen gebruik van de supportprocedure. Om op de rapportages terug te kunnen vinden wie de tools heeft gebruikt, zullen deze support-tools moeten worden gekoppeld aan persoonlijke user-ids. Dit geldt zowel voor nulde-, eerste- als tweedelijnssupport.

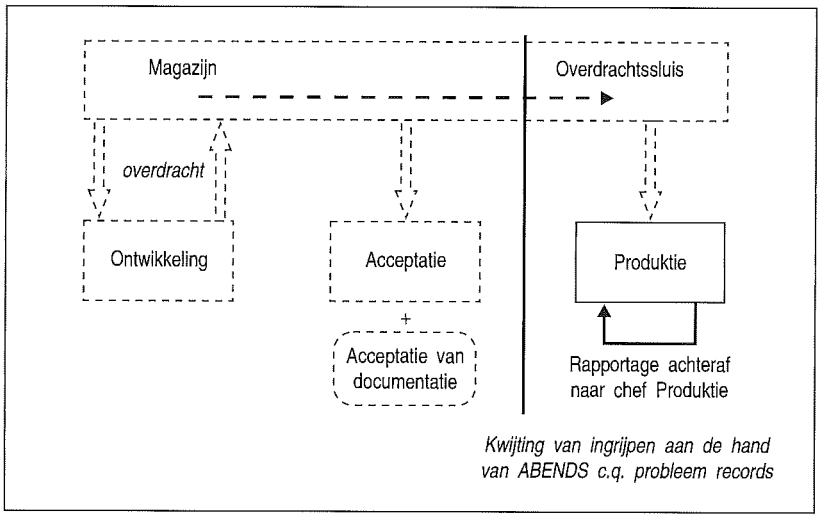
Figuur 10. Autorisatie achteraf na support-verlening van wijzigingen van parameters die buiten *de strekking van de inrichtingsnota vallen.*

De parameters die de afdeling Operations zonder verdere autorisatie mag wijzigen, dienen expliciet te zijn omschreven en te worden gelogd. De rapportage dient gericht te zijn aan de chef Produktie die verantwoordelijk is voor het goed functioneren van de operationele omgeving. Ook rapportages over het onjuiste verloop van jobs ('ABENDS' bijvoorbeeld) en de reden daarvan dienen automatisch te worden vervaardigd en te zijn gericht aan de chef Produktie.

AUDITASPECTEN

Indien de automatiseringsorganisatie met de gebruikersorganisatie een SLA-overeenkomst heeft gesloten, mag de gebruiker ervan uitgaan dat wordt gewerkt met integere programmatuur en data. Hiervoor heeft de VTO infrastructurele middelen aangeschaft (systeemsoftware) en procedures opgesteld die deze integriteit waarborgen. Opdat de EDP-auditor een uitspraak kan doen

2. Indien de eerstelijnssupport wordt verricht door de acceptant vindt hiermee impliciet acceptatie plaats. De rapportage kan worden gebruikt voor een reguliere acceptatie achteraf van de wijzigingen zonder de tijdsdruk van het actuele incident.



Figuur 11. Beheersing van wijzigingen van operationele parameters.

over de mate waarin een organisatie de integriteit van de wijzigingen van software in de produktie-omgeving beheerst, is hieronder een aantal vraagpunten opgesomd. Zo moet worden nagegaan:

- of de functiescheiding tussen ontwikkeling, acceptatie en produktie door de aanwezige middelen en procedures gewaarborgd blijft;
- of alle wijzigingen ('changes') geautoriseerd zijn door de acceptant binnen de VTO;
- of wijzigingen die groter zijn dan de strekking van de inrichtingsnota, geregistreerd zijn door de SO;
- of er geen ongeautoriseerde wijzigingen van de toegangsmatrix of van de functieverdeelstaat door de Security Officer hebben plaatsgevonden;
- of de functionele parameters zijn benoemd en gedocumenteerd in een inrichtingsnota met vermelding van de normatieve waarde en de naam van de registrerende afdeling (SO);
- hoe wordt afgedwongen dat functionele parameters slechts na autorisatie worden gewijzigd. De daarvoor ingestelde procedures en maatregelen moeten naar opzet en werking worden beoordeeld;
- indien gebruik wordt gemaakt van een componentendatabase: in hoeverre de functiescheiding tussen registratie, autorisatie en uitvoering wordt afgedwongen, hoe de registratie wordt bewaakt en in hoeverre van dit instrument gebruik wordt gemaakt;
- of de support wordt verleend met een persoonlijk user-id dat (tijdelijk) gekoppeld is aan een set van support-tools;
- of er rapportages van verleende support plaatsvinden aan de acceptant;
- in hoeverre de rapportages door de acceptant beoordeeld worden;
- of de eerstelijnssupporter inderdaad slechts wijzigingen heeft aangebracht die de strekking van de inrichtingsnota niet overstijgen.

Met de beantwoording van deze vraagpunten kan de EDP-auditor vaststellen dat de eerder beschreven beheersconcepten juist en volledig zijn geïmplementeerd, zodat de conclusie gerechtvaardigd is dat de systeemsoftware onder controle is.

BESLUIT

Wijzigingen van de systeemsoftware-componenten worden het meest optimaal beheerst indien het *overdrachtstraject* wordt doorlopen met scheiding tussen de functies registratie, autorisatie en uitvoering. Bij het doorlopen van het overdrachtstraject vindt expliciete acceptatie van de wijziging *vooraf* plaats. Uit het oogpunt van beheersing wordt dit concept dan ook voor alle wijzigingen van systeemsoftware-componenten gewenst geacht.
Voor wijzigingen die zonder overdrachtstraject rechtstreeks in de produktie-omgeving worden aangebracht, de 'run time'-wijzigingen, is dit

Tabel 1. Beheersconcepten naar soort wijziging.

	Soort wijziging	*Registrerende functie*	*Beschikkende functie*
'Run time' regulier	Wijziging groter dan strekking inrichtingsnota	Wijzigingsaanvraag *vooraf* opstellen door de afdeling Systeem-programmering	Autorisatie *vooraf* door VTO-acceptatie
	Wijziging binnen strekking inrichtingsnota	Wijzigingsaanvraag is impliciet gedocumenteerd in bestaand inrichtingsvoorstel/security-matrix	Autorisatie *vooraf* door VTO-acceptatie
'Run time' incident	Wijziging groter dan strekking inrichtingsnota	Wijzigingsaanvraag *achteraf* opstellen door de afdeling Systeem-programmering aan de hand van rapportage aan SO	Autorisatie *achteraf* door rapportage aan VTO-acceptatie
	Wijziging binnen strekking inrichtingsnota	Wijzigingsaanvraag is impliciet beschreven in bestaand inrichtingsvoorstel/security-matrix	Autorisatie *achteraf* door rapportage aan VTO-acceptatie
Operationele wijziging			Autorisatie *achteraf* door logging aan chef Produktie

beheersingsconcept echter niet toepasbaar. Voor het beheersen van deze wijzigingen moet de functiescheiding (inclusief autorisatie vooraf) procedureel worden geregeld.
Hierbij kan gebruik worden gemaakt van het instrument *componentendatabase*, waarbij de functiescheiding tussen registratie, autorisatie en uitvoering softwarematig wordt afgedwongen. Met name voor wijzigingen van kritieke parameters is dit concept gewenst.

Ten behoeve van het vervullen van de registrerende functie moet onderscheid gemaakt worden in wijzigingen die binnen de strekking van de inrichtingsnota vallen en wijzigingen die verder reiken dan de strekking van de inrichtingsnota.
Voor wijzigingen die binnen de strekking van de inrichtingsnota vallen is de registratie reeds vastgelegd en kan de wijziging rechtstreeks worden geaccepteerd door de acceptant (VTO).
Voor wijzigingen die verder reiken dan de inrichtingsnota dienen de wijzigingsaanvragen te worden opgesteld door de afdeling Ontwikkeling als functioneel beheerder van ontwikkelde en geïmplementeerde software. Na het akkoord van de softwarematige 'vertaling' van de gewijzigde functionaliteit door de afdeling Ontwikkeling dient de acceptant (VTO) de wijziging te accepteren.

Voor wijzigingen van systeemsoftware-componenten bij supportverlening dient autorisatie *achteraf* door de desbetreffende acceptant plaats te vinden aan de hand van de rapportage.
'Run time'-wijzigingen van operationele variabelen worden door Operations ongeautoriseerd aangebracht, waarbij achteraf controle plaats dient te vinden door het hoofd Operations aan de hand van de (loggings)rapportages.

Bij de acceptatie van de software dient ook de documentatie expliciet te worden geaccepteerd. Het is van belang dat alle systeemsoftware-componenten in een inrichtingsnota beschreven staan met vermelding van hun normatieve waarden en vermelding van de acceptant om tot een adequate beheersing van de parameters te kunnen komen.

Geconcludeerd kan worden dat voor elke situatie een beheersingsconcept mogelijk is. Een belangrijke randvoorwaarde voor het adequaat functioneren van de geïmplementeerde beheersingsconcepten is dat het lijnmanagement bereid is tijd te besteden aan de bijbehorende autorisatieprocedures.

LITERATUUR

[Broe93] B.H.J. Broekhuizen, *Waarborging integriteit van overgedragen systeemsoftware*, interne nota ABN AMRO, 1993.

[Hand91] Kluwer, *Handboek EDP Auditing*, deel C.5.11.11, december 1991.

[IBMD] IBM Corporation, *IBM Dictionary of Computing*, SC20-1699.

[ITIL90a] CCTA, *Computer Operations Management*, IT Infrastructure Library, Norwich (GB) 1990.

[ITIL90b] CCTA, *Service Level Management*, IT Infrastructure Library, Norwich (GB) 1990.

[ITIL92] CCTA, *Change Management*, IT Infrastructure Library, Norwich (GB) 1992.

[ITIL93] CCTA, *Problem Management*, IT Infrastructure Library, Norwich (GB) 1993.

[Kock93] C. Kocks, *Inzicht in Samenhang*, syllabus EUR Rotterdam, 1993.

[Koed86] A.H.C. Koedijk e.a., *Database & accountant*, Samsom, Alphen aan den Rijn 1986.

[Looi91] M. Looijen, *EBM Een Beheer Methodiek met SDM*, Cap Gemini Publishing, Rijswijk 1991.

[NGI89] NGI-rapport 4, *Beveiliging bij datacommunicatie*, NGI, Kluwer, Deventer 1989.

[NGI90] *Het organiseren en controleren van het systeembeheer*, rapport van het Nederlands Genootschap voor Informatica, sectie EDP Auditing, maart 1990.

[NIVR21] NIVRA-studierapport 21, *Functiescheidingen in software*, NIVRA, Amsterdam 1988.

[SAC91] SAC Report 4, *Managing Computer Resources*, The Institute of Internal Auditors Research Foundation, Florida, december 1991.

[Völl87] H. Völlmar, *Systeembeheer en beveiliging in de automatisering*, Het Spectrum, Utrecht 1987.

Drs. R.H.H.M. Bronzwaer Is na het voltooien van de studie Bedrijfskunde aan de Erasmus Universiteit Rotterdam sinds 1989 werkzaam als beleidsmedewerker informatiebeveiliging bij de divisie Automatisering van de ABN AMRO Bank. In 1994 heeft hij de post-doctorale studie EDP-auditing aan de EUR voltooid.

Fiscale bewaarplicht van gegevens

T.H.C. van de Molengraft RA

In juli 1994 is de fiscale bewaarplicht van gegevens aangepast aan de moderne tijd. Er blijken bij betrokkenen nog vele onduidelijkheden te bestaan over de toepassing. De fiscale regelgeving en de praktische invulling zoals bijvoorbeeld ten aanzien van conversie worden uiteengezet. Tevens wordt duidelijk aangegeven op welke punten het belangrijk is om vooraf afspraken te maken met de inspecteur.

INLEIDING

Natuurlijke personen en (werknemers van) rechtspersonen onderhouden relaties met vele geledingen van de maatschappij (aandeelhouders, personeel, afnemers, leveranciers, etc.). Binnen die relaties speelt de vastlegging van gegevens een belangrijke rol. De gegevens worden (los van de fiscale bewaarplicht) voor kortere of langere tijd bewaard.
De fiscus is slechts één (meestal niet onbelangrijke) partij.
Om nu te voorkomen dat juist die gegevens die voor de heffing van belastingen essentieel zijn zouden worden vernietigd, is een bewaarplicht opgelegd.

Medewerkers van de Belastingdienst belast met de controle, zullen steeds vaker gebruik gaan maken van digitaal vastgelegde gegevens bij bedrijven.
Voor de bedrijven ligt hierin een belangrijk voordeel. Papieren archieven kunnen door elektronische worden vervangen. Gegevens op een elektronische gegevensdrager nemen minder plaats in dan dezelfde hoeveelheid gegevens op papier. Archiefruimte kan voor andere doeleinden worden gebruikt.
De voordelen voor de Belastingdienst van deze aanpak zijn ook duidelijk: in een zelfde periode kan met meer diepgang worden gecontroleerd en/of de doorlooptijd van de controle wordt korter.
De wettelijke grond voor de vraag om beschikbaarheid van computerbestanden is te vinden in de Algemene Wet inzake Rijksbelastingen (AWR).
Op 14 juli 1994 veranderde de fiscale wetgeving rondom de bewaarplicht van gegevens. De bewaarplicht hangt zeer nauw samen met de ook in de AWR geregelde inlichtingen- en administratieplicht.

In verband met de wetswijziging zond de Staatssecretaris een Notitie aan de Eerste Kamer, waarin hij een aantal uitgangspunten in de nieuwe regelgeving verduidelijkte (Notitie Administratieverplichting en elektronische gegevensverzamelingen, Eerste Kamer, vergaderjaar 1993-1994; 21287 en 21339, nr. 15d).

Ondanks dat de wetswijziging in 1994 is doorgevoerd, zijn nog vele onduidelijkheden over de toepassing te constateren. Accountants en EDP-auditors besteden niet altijd voldoende aandacht aan de (gevolgen van de) wettelijke verplichtingen. Dit artikel beoogt op deze punten wat meer duidelijkheid te verschaffen. Eerst wordt stilgestaan bij de wijzigingen van 1994. Daarna passeren de van belang zijnde wetsartikelen kort de revue en tot slot wordt ingegaan op een aantal vragen over de bewaarplicht die in de praktijk vaak worden gesteld.

VERANDERINGEN IN JULI 1994

In juni 1994 werd wetsontwerp 21287 'Aanpassing van de administratieve verplichtingen' aangenomen door de Eerste Kamer. Op 14 juli 1994 kreeg het ontwerp kracht van wet.
Reeds in 1989 werd een aanzet gegeven tot wijziging van de bewaarplicht. Uitgangspunt is steeds geweest dat voor het bedrijfsleven geen lastenverzwaring mocht optreden. De bewaarplicht als zodanig is dan ook niet uitgebreid. Wel is de terminologie in overeenstemming gebracht met die rond de huidige wijze van administreren. Zo is naast de omschrijving 'boeken en bescheiden' de uitdrukking 'andere gegevensdragers' in de wet opgenomen. Voor juli 1994 kon uit jurisprudentie al worden afgeleid dat ook computerbestanden onder de bewaarverplichting vielen. Thans is elk misverstand op dat punt uitgesloten.

Nieuw in de wet is de mogelijkheid van conversie: de meeste gegevens mogen onder bepaalde voorwaarden van het ene naar het andere medium worden overgebracht. De 'oorspronkelijke' vastleggingen hoeven dan niet meer te worden bewaard. Hier wordt later in dit artikel nog op teruggekomen.

De verantwoordelijkheid voor het bewaren ligt bij de onderneming. Dit is niet nieuw. Nieuw is wel dat de 'bewijslast omkeert' als niet aan de bewaarplicht wordt voldaan.

In de Notitie wordt expliciet de mogelijkheid genoemd om (binnen de wettelijke kaders) afspraken met de inspecteur te maken over onder meer de selectie van de gegevens, op welke wijze die bewaard moeten blijven en hoe ze moeten worden gereproduceerd. In de praktijk biedt dit de mogelijkheid om vooraf zekerheid te krijgen of aan de bewaarplicht wordt voldaan.

FISCALE REGELGEVING

De fiscale administratie- en bewaarplicht is geregeld in de AWR. Ook in andere fiscale wetten (onder meer Omzetbelasting, Loonbelasting, Invorderingswet, Douanewet) zijn nadere regels te vinden. En niet alleen de fiscus geeft regels voor het bewaren van gegevens, ook andere instanties hebben er belang bij. Zo is bijvoorbeeld in het Burgerlijk Wetboek ook een bewaarverplichting opgenomen. Dit artikel gaat overigens alleen in op de fiscale bewaarplicht.

In de volgende subparagrafen wordt ingegaan op de wettelijke kaders.

Inlichtingenplicht

De bewaarplicht hangt nauw samen met de inlichtingenplicht. Iedere belastingplichtige heeft een inlichtingenplicht jegens de inspecteur.

Artikel 47 lid 1 van de AWR luidt:

'Ieder is gehouden desgevraagd aan de inspecteur
a. de gegevens en inlichtingen te verstrekken welke voor de belastingheffing te zijnen aanzien van belang kunnen zijn;
b. boeken, bescheiden en andere gegevensdragers of de inhoud daarvan – zulks ter keuze van de inspecteur – waarvan de raadpleging van belang kan zijn voor de vaststelling van de feiten, welke invloed kunnen uitoefenen op de belastingheffing te zijnen aanzien, voor dit doel beschikbaar te stellen.'

Deze inlichtingenplicht leidt niet automatisch tot een bewaarplicht.
De bewaarplicht is alleen opgelegd aan administratieplichtigen. Alle belastingplichtigen hebben een inlichtingenplicht, niet allemaal hebben ze een bewaarplicht.
Wie als administratieplichtig wordt beschouwd, wordt in de volgende subparagraaf besproken.

De inlichtingenplicht leidt niet automatisch tot een bewaarplicht.

Wie moet bewaren?

Het antwoord op deze vraag is te vinden in artikel 52.

Artikel 52 lid 2 luidt:
'Administratieplichtig zijn:
a. lichamen;
b. natuurlijke personen die een bedrijf of zelfstandig beroep uitoefenen;
c. natuurlijke personen die inhoudingsplichtig zijn.'

En artikel 52 lid 4:
'Administratieplichtigen zijn verplicht de in de voorgaande leden bedoelde informatiedragers gedurende 10 jaren te bewaren.'

De conclusie die hieruit getrokken kan worden, is dat natuurlijke personen die geen onderneming of zelfstandig beroep uitoefenen of inhoudingsplichtig zijn, informatiedragers niet hoeven te bewaren. Zij moeten echter wel als de inspecteur daarom vraagt, gegevens en inlichtingen verschaffen ten aanzien van hun eigen aangifte (artikel 47 lid 1).
Het is dus wel onverstandig om informatiedragers te vernietigen, die bijvoorbeeld bij het aantonen van kosten behulpzaam kunnen zijn.

Wat moet worden bewaard?

Administratieplichtigen moeten een administratie bijhouden volgens artikel 52 lid 1:
'Administratieplichtigen zijn gehouden van hun vermogenstoestand en van alles betreffende hun bedrijf, zelfstandig beroep of werkzaamheid naar de eisen van dat bedrijf, dat zelfstandig beroep of die werkzaamheid op zodanige wijze een administratie te voeren en de daartoe behorende boeken, bescheiden en andere gegevensdragers op zodanige wijze te bewaren, dat te allen tijde hun rechten en verplichtingen alsmede de voor de heffing van

belasting overigens van belang zijnde gegevens hieruit duidelijk blijken.'

Artikel 52 lid 3 vermeldt dat ook datgene wat wordt bijgehouden op grond van andere belastingwetten tot de administratie behoort. Hierbij kan bijvoorbeeld worden gedacht aan de loonstaten die volgens artikel 25 van de Uitvoeringsregeling Loonbelasting moeten worden aangelegd.

Artikel 52 lid 4 spreekt over *'de in de voorgaande leden bedoelde gegevensdragers'*.

De gegevensdragers hebben voor de fiscus in het algemeen betekenis door de gegevens die erop zijn weggeschreven. De gegevens waar het hier om gaat maken deel uit van de administratie.

Welk medium?

De administratieplichtige is in beginsel vrij in de keuze om de gegevens op papier of op een ander medium te bewaren. Alleen de balans en resultatenrekening moeten beslist op papier worden bewaard. De administratieplichtige mag gegevens onder bepaalde voorwaarden omzetten (converteren) van het ene naar het andere medium (bijvoorbeeld van papier naar een scanbestand op een diskette). In dit verband zijn twee leden van artikel 52 van belang, te weten artikel 52 lid 5, dat luidt:
'De op een gegevensdrager aangebrachte gegevens, uitgezonderd de op papier gestelde balans en staat van baten en lasten, kunnen op een andere gegevensdrager worden overgebracht en bewaard, mits de overbrenging geschiedt met juiste en volledige weergave der gegevens en deze gegevens gedurende de volledige bewaartijd beschikbaar zijn en binnen redelijke tijd leesbaar kunnen worden gemaakt.'

Alleen de balans en resultatenrekening moeten beslist op papier worden bewaard.

en artikel 52 lid 6, dat luidt:
'De administratie dient zodanig te zijn ingericht en te worden gevoerd en de gegevensdragers dienen zodanig te worden bewaard, dat controle daarvan door de inspecteur binnen een redelijke termijn mogelijk is. Daartoe verleent de administratieplichtige de benodigde medewerking met inbegrip van het verschaffen van het benodigde inzicht in de opzet en werking van de administratie.'.

Deze twee leden van artikel 52 vormen de kern van de nieuwe bewaarplicht. Hierin is geregeld dat alle gegevens in beginsel nog maar één keer hoeven te worden bewaard, en wel op een medium van eigen keuze.
De beperking in de keuze komt tot uiting in de vereiste garantie dat overbrenging juist en volledig moet geschieden (lid 5) en de eis dat controle binnen een redelijke termijn mogelijk moet zijn (lid 6).

Relatie tussen medium en gegevens

De Belastingdienst heeft belang bij de gegevens. In een 'papieren' omgeving zijn medium en gegevens vaak een onlosmakelijk geheel. Op het moment dat de inspecteur de boeken/bescheiden ter inzage ontvangt, kan hij ook kennis nemen van de inhoud ervan (mits hij de gebezigde taal machtig is).

Met de vastlegging in digitale vorm is het rechtstreekse verband tussen het medium en de gegevens losgelaten. Ook al wordt het medium ter inzage verstrekt (bijvoorbeeld een diskette) dan nog is de inhoud van de gegevens niet zonder meer leesbaar. Daarom is in artikel 47 lid 1 letter b, opgenomen *'boeken, bescheiden en andere gegevensdragers of de inhoud daarvan'* en in artikel 52 lid 6 dat de administratieplichtige medewerking moet verlenen aan de controle.

Gegevensdragers bij derden

Soms wordt gebruik gemaakt van de diensten van servicebureaus. Gesteld zou kunnen worden dat de daar gebruikte gegevensdragers geen eigendom zijn van de belastingplichtige en dat ze om die reden niet ter inzage kunnen worden gegeven. De inspecteur kan in zo'n geval een beroep doen op artikel 48:
'1. De in artikel 47, eerste lid, onderdeel b, bedoelde verplichting geldt onverminderd voor een derde bij wie zich gegevensdragers bevinden van degene die gehouden is deze, of de inhoud daarvan, aan de inspecteur voor raadpleging beschikbaar te stellen.
2. De inspecteur stelt degene wiens gegevensdragers hij bij een derde voor raadpleging vordert, gelijktijdig hiervan in kennis.'

Andere ambtenaren belastingdienst

In de hierboven aangehaalde AWR-artikelen worden verplichtingen jegens de inspecteur opgesomd. Dezelfde verplichtingen gelden ook jegens andere (aangewezen) belastingambtenaren op grond van artikel 56 AWR:
'De verplichtingen welke volgens deze afdeling bestaan jegens de inspecteur, gelden mede jegens iedere door of vanwege Onze Minister aangewezen andere ambtenaar van de rijksbelastingdienst.'

In dit kader zijn controlemedewerkers van de Belastingdienst aangewezen ambtenaren.

Sancties

De verantwoordelijkheid voor het bewaren ligt bij de administratieplichtige. Binnen de wettelijke kaders is deze vrij in het bepalen wat wordt bewaard en op welke manier.
Soms blijkt dat niet alle vereiste gegevens bewaard zijn gebleven. Tenzij sprake is van overmacht kan de administratieplichtige worden geconfronteerd met de volgende sancties:
- omkering van de bewijslast;
- strafrechtelijke vervolging.

De omkering van de bewijslast is geregeld in artikel 54:
'De administratieplichtige die niet of niet volledig voldoet aan de vordering gegevensdragers, of de inhoud daarvan, voor raadpleging beschikbaar te stellen, wordt voor de toepassing van de artikelen 25 en 29 geacht niet volledig te hebben voldaan aan een bij of krachtens artikel 52 opgelegde verplichting, tenzij aannemelijk is dat de afwezigheid of onvolledigheid van de gegevensdragers of de inhoud daarvan het gevolg is van overmacht.'

In artikel 68 lid 1 wordt het niet voldoen aan de hiervoor omschreven eisen als strafbaar feit aangeduid. In het kader van dit artikel wordt hier niet verder op ingegaan, het uitgangspunt in dit artikel is immers hoe wel aan de vereisten kan worden voldaan.

PRAKTISCHE INVULLING VAN DE BEWAARPLICHT

In gesprekken met administratieplichtigen over de fiscale bewaar- en inlichtingenplicht komen vaak dezelfde vragen naar voren. Alvorens op een aantal van die vragen in te gaan, wordt het onderscheid beschreven tussen interne en externe vastleggingen en dat tussen vaste en variabele gegevens. Het onderscheid tussen de verschillende begrippen is van belang bij de keuze hoe gegevens bewaard moeten blijven.

Interne versus externe vastleggingen

Onder interne vastleggingen worden al die vastleggingen verstaan die voortkomen uit de eigen bedrijfsvoering. Onder externe vastleggingen vallen alle gegevens die van buiten de onderneming worden aangereikt. Bijvoorbeeld: alle gegevens op een verkoopfactuur volgen uit interne vastleggingen. In een geautomatiseerde omgeving betekent dit, dat de vermelde gegevens ergens in de systemen aanwezig zijn op het moment dat de factuur wordt aangemaakt.
In AWR-termen kan worden gesteld dat bij het afdrukken van de factuur digitale gegevens worden geconverteerd naar papier. Wanneer nu de digitale gegevens samen met een voorbeeldfactuur juist en volledig worden bewaard, kunnen facturen altijd weer worden ge(re)produceerd.
Gegevens op een inkoopfactuur worden gezien als extern. Vaak worden alleen de gegevens die noodzakelijk zijn voor de eigen bedrijfsvoering in de eigen administratie overgenomen. Een voorbeeld van een gegeven op een inkoopfactuur dat zelden wordt opgenomen in de eigen administratie, is een logo.

Vaste gegevens versus variabele gegevens

Vaste gegevens verdienen bij het bewaren extra aandacht. Vaste gegevens (of stamgegevens) zijn die gegevens die veelvuldig binnen een systeem worden gebruikt. De waarde ervan kan in de tijd weliswaar veranderen maar doet dit relatief zeer weinig. Tegenover de vaste gegevens staan de variabele gegevens. Deze worden eenmalig voor een transactie gebruikt en veranderen daarna niet meer. Bijvoorbeeld naam-, adres- en woonplaatsgegevens van een afnemer kunnen als vast gegeven worden aangemerkt, de aantallen geleverde artikelen worden als variabel aangemerkt.
Stamgegevens worden bij een mutatie ervan nog vaak overschreven: de oude waarden worden weggegooid, de nieuwe waarden komen ervoor in de plaats.

De administratieplichtige zal maatregelen moeten treffen om ook de (verouderde) stamgegevens volledig en juist te bewaren.

Bijvoorbeeld: het oude adres van een afnemer wordt 'overschreven' met diens nieuwe adres. Verkoopfacturen komen vanaf dat moment op het juiste adres aan. Echter, indien de inspecteur bij de controle oudere verkoopfacturen wenst te reproduceren, kan het voorkomen dat die facturen het nieuwe adres vermelden. Dit is niet juist.
De administratieplichtige zal maatregelen moeten treffen om ook de (verouderde) stamgegevens volledig en juist te bewaren.
In de Notitie wordt een drietal mogelijkheden beschreven waarmee aan de bewaarplicht kan worden voldaan:

– *Het opnemen van een tijdselement*
Als een afnemer bijvoorbeeld is verhuisd, wordt een 'einddatum' bij de gegevens van die debiteur ingevuld. Vervolgens wordt die debiteur met het nieuwe adres en de 'ingangsdatum' aan het bestand toegevoegd.

– *Vaste gegevens vastleggen bij de transactie*
Bij het opslaan van verkoopgegevens wordt bijvoorbeeld per factuur niet alleen het debiteurennummer opgeslagen maar ook de naam-, adres- en woonplaatsgegevens.

– *Was/wordt-rapportage*
Uit het oogpunt van interne controle worden mutaties in vaste gegevens vaak zichtbaar gemaakt in een was/wordt-rapportage. Om aan de bewaarplicht te voldoen moeten deze rapporten dan wel in digitale vorm worden bewaard.

Men voldoet pas aan de bewaarplicht indien in ieder geval de stamgegevens juist en volledig bewaard blijven.

Initiatief tot overleg

De verantwoordelijkheid voor het bewaren van gegevens ligt bij de administratieplichtige. De fiscus gaat ervan uit dat alle gegevens bewaard blijven en dat ze binnen een redelijke termijn leesbaar en controleerbaar zijn.
Vaak wordt de bewaarplicht ter sprake gebracht in

een 'bedrijfsgesprek' of tijdens een boekenonderzoek. Soms neemt de administratieplichtige contact op met de fiscus op het moment dat een nieuw systeem wordt aangeschaft.
Het komt ook voor dat een architect zijn opdrachtgever naar de fiscus verwijst. Het is zelfs voorgekomen dat na overleg de geplande extra archiefruimte kon vervallen. Ook leveranciers van software nemen soms contact op met de inspecteur. Dit gebeurt meestal naar aanleiding van vragen van hun afnemers.
Het is uitermate belangrijk dat leveranciers goed op de hoogte zijn van de fiscale eisen ten aanzien van de bewaar- en inlichtingenplicht. Bij de ontwikkeling en het onderhoud van software kan dan rekening worden gehouden met die eisen. Het zijn echter de afnemers die verantwoordelijk zijn en blijven voor het nakomen van de wettelijke verplichtingen.

Systeemdocumentatie van hard- en software valt ook onder de bewaarplicht.

Rol van accountant en EDP-auditor

Tot op heden wordt door accountants en EDP-auditors in veel gevallen nog onvoldoende aandacht besteed aan de fiscale bewaarplicht. Het is van groot belang dat zij hun opdrachtgevers wijzen op (de gevolgen van) de wettelijke regels rondom de bewaarplicht. In de praktijk merkt een administratieplichtige nog te vaak op dat zijn adviseur gezegd heeft dat het bewaren van alle gegevens op papier wel voldoende is. Overleg tussen opdrachtgever, adviseur en fiscus voorkomt misverstanden op dit punt.

Nieuwe hardware en/of software

De (economische) levensduur van hard- en software is meestal korter dan de tien jaren van de bewaarplicht. Administratieplichtigen vragen dan ook vaak of de bewaarplicht van digitale gegevens leidt tot het in de lucht moeten houden van alle oorspronkelijke hard- en software gedurende tien jaar.
Het antwoord op deze vraag is in beginsel 'nee'. De fiscus is primair geïnteresseerd in de gegevens. Indien de gegevens los van de oude systemen binnen een redelijke termijn benaderbaar zijn en blijven, hoeven die oude systemen niet operationeel te blijven. Het gaat er dan om dat gegevens in een leesbare vorm worden weggeschreven naar 'systeemonafhankelijke' gegevensdragers.
Nu zou opgemerkt kunnen worden dat dit altijd al gebeurde. Het is immers niet ongebruikelijk dat elektronisch vastgelegde gegevens op papier worden afgedrukt alvorens de elektronische versies worden vernietigd. En papier is systeemonafhankelijk.
Toch voldoet men dan niet meer aan de bewaarplicht. Dit wordt in de subparagraaf Conversie nader toegelicht.

Voor alle duidelijkheid: systeemdocumentatie van (vervangen) hard- en software behoort tot de administratie en valt als zodanig ook onder de bewaarplicht.

Systeemgerichte onderzoeken

Hierboven werd opgemerkt dat de fiscus primair is geïnteresseerd in gegevens. Hieruit mag niet worden geconcludeerd dat alleen maar gegevensgericht wordt gecontroleerd. De Belastingdienst kan en mag systeemgerichte onderzoeken instellen. In de Notitie is overigens geschreven dat systeemtoetsen alleen op operationele systemen kunnen worden uitgevoerd. Een verdere beschrijving van de aanpak valt buiten het bestek van dit artikel.

Redelijke termijn

Controle moet volgens artikel 52 lid 6 AWR binnen een redelijke termijn mogelijk zijn. De vraag is wat in dit verband een 'redelijke' termijn is.
Dit is afhankelijk van de omstandigheden. Wanneer bijvoorbeeld een boekenonderzoek enkele weken tevoren wordt aangekondigd, mag worden verwacht dat de gegevens bij aanvang van het onderzoek in de door de controlemedewerker gewenste vorm beschikbaar zijn. Als de periode tussen aankondiging en eerste bezoek korter is, zal wellicht nog in redelijkheid gevraagd kunnen worden naar (digitaal vastgelegde) gegevens van de laatst afgesloten periode.
Het is verstandig om in geval van twijfel afspraken te maken met de inspecteur over welke termijn in specifieke gevallen redelijk te noemen is.

Conversie

De mogelijkheid van conversie is in 1994 in de AWR opgenomen. Het afdrukken van digitaal vastgelegde gegevens naar papier valt onder het begrip conversie. Toch is het bewaren van de afgedrukte gegevens alleen in de meeste gevallen niet voldoende. Ook mogen bij conversie geen gegevens verloren gaan of veranderen.

Naar papier
Toen geheugencapaciteit nog schaars was, was het gebruikelijk om telkens na afloop van een periode de gegevens naar (papieren) lijsten af te drukken. Vervolgens kon de vrijgekomen geheugenruimte weer worden gebruikt voor een nieuwe periode. Deze vorm van conversie (van digitaal naar papier) is nu vrijwel altijd in strijd met de wettelijke verplichtingen. Alleen bij eenmanszaken is deze vorm van conversie nog toegestaan.
De administratie wordt niet voor niets geautomatiseerd gevoerd. Gegevens worden daarmee over het algemeen beter en sneller toegankelijk voor de bedrijfsvoering. Het komt dan ook steeds vaker voor dat de bedrijfsvoering in gevaar komt zodra een geautomatiseerd systeem voor kortere of langere tijd uitvalt.
In artikel 52 lid 6 is de eis geformuleerd dat de gegevens zodanig moeten worden bewaard dat controle daarvan binnen een redelijke termijn

mogelijk is. Als nu het geautomatiseerde systeem zo goed als onmisbaar is voor de bedrijfsvoering dan is controle vanaf papier niet binnen een redelijke termijn mogelijk. Om deze reden is het niet toegestaan gegevens te converteren van digitaal naar papier.

Volledig en juist
Alvorens de originele gegevens kunnen worden vernietigd, zal moeten worden vastgesteld dat de conversie volledig en juist is geweest. Met andere woorden, er mogen geen gegevens verloren gaan en de gegevens moeten juist worden geconverteerd. De garantie voor volledigheid en juistheid moet verankerd zijn in de administratieve organisatie. Het mag natuurlijk niet voorkomen dat originelen worden vernietigd terwijl sommige gegevens wel en andere weer niet naar een nieuwe gegevensdrager zijn geconverteerd. In de praktijk betekent dit dat in kleinere organisaties met beperkte controletechnische functiescheidingen, gegevens toch vaak nog 'dubbel' bewaard moeten blijven. Inkoopfacturen mogen dan bijvoorbeeld niet worden vernietigd na conversie naar een scanbestand omdat de administratieve organisatie onvoldoende waarborgen biedt voor de volledigheid van het inkoopfacturenbestand. Het scanbestand mag niet worden vernietigd, omdat daarmee de mogelijkheid van een controle binnen een redelijke termijn geweld wordt aangedaan.

Juiste moment
Van groot belang is het juiste moment van conversie. Scant men bijvoorbeeld een inkoopfactuur voordat het blokstempel (met voor de controle relevante aantekeningen) is ingevuld, dan dient zowel de scan als de originele factuur met het ingevulde blokstempel te worden bewaard. Beter zou zijn als wordt gewacht met inscannen totdat de factuur het interne-controletraject heeft doorlopen. Het te vroeg scannen leidt tot een 'onvolledige' conversie. De administratieplichtige kan vooraf zekerheid krijgen over het juiste moment door een afspraak hierover met de fiscus te maken.

Tussenbestanden

Vaak worden (al dan niet zichtbare) 'tussenbestanden' aangemaakt. Deze worden dan na gebruik door de programmatuur weer verwijderd. Strikt formeel vallen ook deze bestanden onder de bewaarplicht. In de Notitie is echter aangegeven dat deze bestanden niet bewaard hoeven te blijven.

Mate van detaillering

Er worden steeds meer gegevens in administraties verwerkt. De hardware en de geheugencapaciteit leggen hieraan in principe geen beperking meer op.
De bewaarplicht gaat echter heel ver: die gegevens moeten allemaal bewaard blijven. Het lijkt niet zinvol om de administratieplichtige te belasten met een bewaarplicht, als direct duidelijk is dat de fiscus nimmer zal vragen naar de gegevens. Het is dan verstandig wel van tevoren een afspraak te maken met de inspecteur.

Een voorbeeld ter verduidelijking. Voor de bedrijfsvoering van een kledingzaak met een aantal filialen is het van belang te weten in welk filiaal een bepaalde maat en/of kleur van een kledingstuk aanwezig is. De administratie wordt daarop ingericht. Behalve in het geval dat verkoopprijzen ook afhankelijk zijn van maat en/of kleur zal het niet of zeer zelden voorkomen dat de inspecteur de maat- en kleurgegevens nodig heeft om tot een juiste en verantwoorde belastingheffing te komen.
De ondernemer zou in dit voorbeeld een afspraak met de inspecteur kunnen maken om de voorraadmutaties per model te bewaren.

Op grond van de AWR kan de controlemedewerker kiezen hoe hij de gegevens ter beschikking wil krijgen.

Produktie van gegevens

Stel nu dat conform de hierboven geschetste uitgangspunten 'alle' gegevens zijn bewaard. Hoe kan de controlemedewerker dan gebruik gaan maken van de digitaal vastgelegde gegevens?
Op grond van artikel 47 lid 1 letter b van de AWR kan de controlemedewerker kiezen hoe hij de gegevens ter beschikking wil krijgen. Daarbij bestaan onder meer de volgende mogelijkheden:
- de gegevens worden in de gewenste vorm op/door het systeem van de administratieplichtige zichtbaar gemaakt (bijvoorbeeld op een terminal);
- de gegevens worden in digitale vorm aangeleverd op een gegevensdrager (bijvoorbeeld diskette, tape of CD). De gegevens worden vervolgens op apparatuur van de Belastingdienst met eigen auditsoftware benaderd.

Gegevens van het laatste jaar of de laatste paar jaren kunnen meestal zonder veel problemen elektronisch worden benaderd. Anders wordt het met oudere gegevens. Daarbij doen zich allerlei praktische problemen voor. Het systeem kan dan bijvoorbeeld onvoldoende vrije ruimte hebben om backups uit oudere jaren terug te zetten of oude software blijkt niet meer te functioneren in de huidige omgeving.

Vaak wordt dan de gegevensdrager met de (back-up)-bestanden aangeboden met de mededeling 'hier staat op wat gevraagd is'. Daarmee zou aan de wettelijke verplichtingen kunnen zijn voldaan onder twee voorwaarden. De gegevensdrager moet in technische zin benaderbaar zijn en de gegevens op de gegevensdrager moeten benaderbaar zijn. Een tweetal voorbeelden:
- op een tape die is aangemaakt met een zeldzaam merk tapestreamer, kunnen wel alle gegevens staan, maar zonder die streamer zijn ze niet benaderbaar;
- gegevens die zijn weggeschreven volgens een

T.H.C. van de Molengraft RA Is werkzaam als EDP-auditor bij de Belastingdienst Grote Ondernemingen Eindhoven. In 1994 heeft hij de post-doctorale opleiding EDP-Audit aan VU Amsterdam afgerond. Dit artikel is geschreven op persoonlijke titel.

geheel aan de gebruikte software eigen structuur zijn zonder die software niet benaderbaar. Gegevens(dragers) bewaren die niet meer benaderbaar zijn, is niet alleen niet zinvol maar bovendien in strijd met artikel 52 lid 1.

Attentiepunten

Het is in het belang van zowel de administratieplichtige als de fiscus dat gegevens digitaal worden bewaard en uitgewisseld. Simpelweg bewaren is op zich nog niet voldoende om tot een succesvolle uitwisseling te komen. De benaderbaarheid moet ook adequaat geregeld zijn. Attentiepunten daarbij zijn:

- Bij vervanging van apparatuur zullen gegevens op gegevensdragers van de oude apparatuur moeten worden geconverteerd naar nieuwe gegevensdragers. Pas daarna kan de oude apparatuur worden weggedaan.

- Het verdient aanbeveling om gegevens onafhankelijk van gebruikte software op te slaan (bijvoorbeeld in platte ASCII-bestanden). Daarmee wordt voorkomen dat bij vervanging van (een versie van) de software telkens alle oude gegevens moeten worden omgezet. De voorschriften eerder genoemd in de subparagraaf Conversie dienen hierbij uiteraard in acht te worden genomen.

- Per bestand moeten ook het aantal records en de lay-out worden bewaard.

- Van oudere gegevensdragers is bekend dat ze na verloop van tijd minder betrouwbaar worden. Gegevens op tapes bijvoorbeeld kunnen na verloop van een paar jaren onleesbaar worden. Het jaarlijks 'refreshen' kan dit voorkomen.

- Gegevensdragers zullen op een plaats moeten worden bewaard waar ze beschermd zijn tegen schadelijke invloeden van de omgeving. Tapes of diskettes die in een vochtige schuur worden bewaard, zullen de gegevens zeker binnen tien jaar verliezen.

Beveiliging

Gegevens in digitale vorm hebben in vergelijking met die op papier een hoge dichtheid. Een diskette kan gegevens van vele vellen papier bevatten. Met de juiste apparatuur en programmatuur zijn die gegevens sneller en beter toegankelijk. Dit alles vereist extra aandacht voor de beveiliging van elektronisch aangeleverde gegevens, omdat ook kwaadwillenden op die manier snel over veel vertrouwelijke gegevens zouden kunnen beschikken. De extra aandacht geldt niet alleen van de administratieplichtige, maar ook van de Belastingdienst. De Belastingdienst staat borg voor de beveiliging van de aangeleverde gegevens. Gelukkig schenken steeds meer bedrijven ook voldoende aandacht aan de beveiliging van hun gegevens.

SAMENVATTING

Medio 1994 is de regelgeving rondom de bewaarplicht aangepast aan de stand van de techniek en jurisprudentie op dat moment. Aan de oude termen 'boeken' en 'bescheiden' is de term 'andere gegevensdragers' toegevoegd en de mogelijkheid van conversie is in de wet opgenomen.
Personen en lichamen die administratieplichtig zijn moeten boeken, bescheiden en andere gegevensdragers bewaren om ze desgevraagd aan de inspecteur ter beschikking te stellen. Ze zijn niet vrij in de keuze van de manier en het medium waarop de gegevens worden bewaard. Bij die keuze moet uitdrukkelijk rekening worden gehouden met de eisen dat de gegevens binnen een redelijke termijn leesbaar en controleerbaar moeten zijn.
Elektronisch vastgelegde gegevens moeten hoe dan ook in die vorm bewaard blijven. Het alleen bewaren van afdrukken op papier van die gegevens is onvoldoende. Accountants en EDP-auditors zullen bij hun onderzoeken aandacht moeten besteden aan de wettelijke regels en zo nodig hun opdrachtgevers wijzen op tekortkomingen.
Afspraken met de inspecteur binnen de wettelijke kaders en uitgangspunten kunnen vooraf zekerheid bieden voor de administratieplichtige of aan de bewaarplicht wordt voldaan.

System Review Services

Mw. drs. M.J.A. Koedijk RA en
mw. W.A. de Munck RA

System Review Services (SRS) biedt de mogelijkheid om op efficiënte wijze met behulp van een definitie van de risico's die de doelstellingen van bedrijfsprocessen bedreigen, de betrouwbaarheid van informatiesystemen te beoordelen. Door middel van een procesgerichte benadering wordt voldoende inzicht verkregen in de functionaliteit van de systemen en de wijze waarop de systemen de bedrijfsprocessen ondersteunen en kunnen heldere eisen van interne controle worden gesteld aan de informatiesystemen. Op basis van deze eisen kan de effectiviteit van getroffen (of te treffen) maatregelen van interne controle eenvoudig worden beoordeeld.

INLEIDING

Informatietechnologie speelt bij het besturen van ondernemingen en bij het beheersen van risico's een steeds grotere rol. Uit effectiviteits- en efficiency-overwegingen worden administratieve procedures en maatregelen van interne controle in toenemende mate geautomatiseerd. Voorbeelden hiervan zijn:

- geprogrammeerde controles op de juistheid of waarschijnlijkheid van invoergegevens op het moment van invoer, in plaats van handmatige controle na de verwerking met behulp van mutatieverslagen of zogenaamde was/wordt-lijsten;
- automatische matching van inkoopfacturen met de geplaatste order en de goederenontvangst in plaats van een integrale handmatige controle zodat door de administratie uitsluitend niet-acceptabele verschillen behoeven te worden uitgezocht.

Dit impliceert dat gebruikers voor hun maatregelen van interne controle in toenemende mate afhankelijk worden van automatisering. De gecompliceerde automatiseringstechnologie vormt voor gebruikers echter, vanuit hun vaak niet technische achtergrond, een belemmering om voldoende inzicht te krijgen in de wijze waarop de geautomatiseerde gegevensverwerking wordt beheerst. Het systeem blijft een zwarte doos zodat het risico ontstaat dat systeemfuncties en geautomatiseerde maatregelen verkeerd worden geïnterpreteerd, waardoor wel noodzakelijke gebruikerscontroles achterwege blijven.

In het kader van de jaarrekeningcontrole zal de hedendaagse accountant willen steunen op de wijze waarop de ondernemingsleiding de bedrijfsrisico's beheerst. De toenemende graad van automatisering van de bedrijfsprocessen en het koppelen van logistieke systemen met financiële systemen versterken de conclusie dat de accountant inzicht dient te krijgen in de betrouwbaarheid van de kritieke geautomatiseerde systemen ([Munc95]).
Hierbij loopt de accountant tegen hetzelfde probleem aan als de gebruikers. Onvoldoende inzicht in en begrip van de functionaliteit van de systemen bij de cliënt dwingen de accountant tot een controlebenadering die in belangrijke mate gegevensgericht is.

Een sterk functioneel en procesgerichte systeembeoordelingsmethodiek als System Review Service (SRS) biedt de gebruiker en de accountant, maar ook andere functionarissen met beperkte technische kennis die zich een beeld willen vormen van de betrouwbaarheid van geautomatiseerde gegevensverwerking, een gestructureerde benadering die hen in staat stelt een effectieve en efficiënte systeembeoordeling uit te voeren.
SRS is vanuit de praktijk ontwikkeld binnen KPMG-internationaal. Het is een beproefde methodiek die zich in de praktijk heeft bewezen. Dit artikel geeft inzicht in achtereenvolgens het object van beoordeling, de fasering en de toepasbaarheid van SRS.

OBJECT VAN BEOORDELING MET BEHULP VAN SRS

De betrouwbaarheid van een IT-systeem wordt grotendeels bepaald door computercontroles met een algemeen karakter (de general IT controls of algemene computercontroles; zie figuur 1 en [Munc95]), en computercontroles die zich richten op de betrouwbare werking van een specifieke applicatie (de application controls of toepassingscontroles).

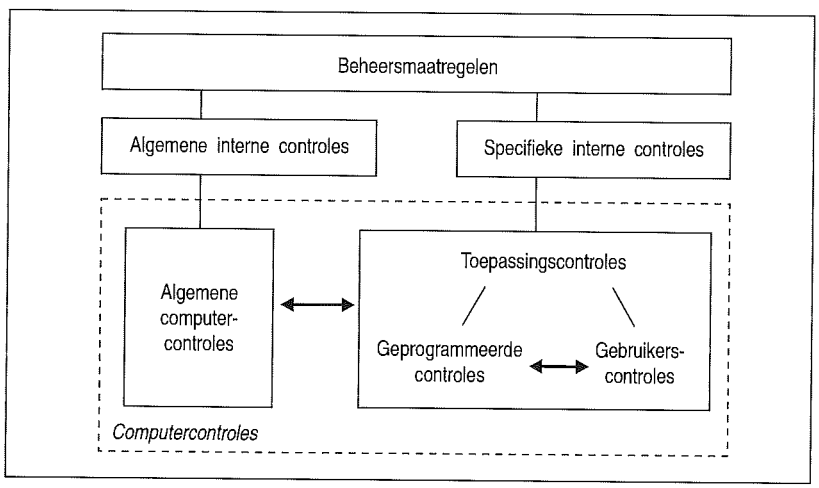
- Beleid en management
- Functiescheidingen
- Logische toegangsbeveiliging
- Fysieke toegangsbeveiliging
- Systeemontwikkeling en onderhoudsprocedures
- Continuïteit
- Systeembeheer- en rekencentrumprocedures
- Gebruikerssatisfactie

Figuur 1. Algemene computercontroles.

De opzet van de algemene computercontroles is geen specifiek object van onderzoek met behulp van de SRS-methodiek. Dat neemt niet weg dat ten behoeve van een uiteindelijk oordeel omtrent de goede werking van een systeem de algemene beheersmaatregelen een belangrijke rol spelen.
Zo zal bijvoorbeeld de goede werking van geprogrammeerde controles worden ondersteund door de kwaliteit van de systeemontwikkelings- en onderhoudsprocedures (met inbegrip van test-, acceptatie- en overdrachtsprocedures). Zij kunnen immers waarborgen dat de geprogrammeerde controles werken zoals volgens de specificaties van de gebruikers wordt verondersteld. Dit is zeker van belang indien de betrouwbaarheid van de geautomatiseerde gegevensverwerking in belangrijke mate wordt beheerst door geprogrammeerde controles.

De algemene beheersmaatregelen kunnen worden beoordeeld met behulp van onder meer rekencentrumaudits, specifieke beveiligingsonderzoeken en onderzoeken die in het kader van de jaarrekeningcontrole moeten plaatsvinden.

Figuur 2. Samenhang beheersmaatregelen.



Figuur 2 geeft inzicht in de samenhang tussen de algemene beheersmaatregelen en de toepassingscontroles.

De toepassingscontroles vormen het specifieke object van onderzoek bij het gebruik van de SRS-methodiek. Dit geldt voor zowel de geprogrammeerde controles als de gebruikerscontroles. Dit impliceert dat het begrip systeem als beoordelingsobject binnen SRS ruim wordt geïnterpreteerd als zijnde de functionaliteit binnen de applicaties met inbegrip van het voor- en natraject in de gebruikersorganisatie.

DE FASERING VAN SRS

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 op basis van te beheersen risico's;
6. inventarisatie en evaluatie van beheersmaatregelen;
7. rapportage.

De SRS-methodiek zal per fase worden toegelicht.

Opdrachtformulering

Systeembeoordelingen kunnen plaatsvinden in opdracht van het management van de onderneming of in het kader van de controle van de jaarrekening. Het is in beide gevallen van belang dat in de opdrachtformulering aandacht wordt geschonken aan het doel en object van het onderzoek, de scope (reikwijdte), de doorlooptijd, de verwachte kosten, de randvoorwaarden en het eindprodukt (rapportage).

Met name een heldere definitie van de scope is van groot belang om verkeerde verwachtingen bij de opdrachtgever te voorkomen. Tijdens de opdrachtformulering moet duidelijk worden welke (gedeelten van de) systemen beoordeeld zullen worden. Bij de omschrijving van het object van onderzoek mag geen ruimte voor misinterpretatie ontstaan. Aspecten die daarbij aandacht verdienen zijn:

– Een duidelijke typering van de te beoordelen systeemfuncties of systemen. Het is niet noodzakelijk dat een geheel systeem object van onderzoek is. Zeker in het geval van specifieke problemen bij een cliënt of in het kader van de controle van de jaarrekening kan het onderzoek zich beperken tot de systeemfuncties die een bijdrage leveren aan de beheersing van de daarvoor relevante risico's.

– Helderheid omtrent de mate waarin interfaces naar of van andere systemen wel of niet in het onderzoek worden betrokken. Hierbij moet de uiteindelijke doelstelling van het onderzoek bepalend

zijn voor de keuze of een interface wel of niet binnen het object van onderzoek valt.

Eveneens moet duidelijk worden of het onderzoek is beperkt tot een oordeel omtrent de opzet en het bestaan van de maatregelen in het systeem of dat ook een uitspraak wordt verlangd omtrent de werking van de maatregelen in het systeem. Tevens moet in de vastlegging van de scope helderheid worden verschaft of een oordeel over de algemene beheersmaatregelen (zie eerder in dit artikel) wordt gegeven.

SRS-onderzoeken richten zich in de regel hoofdzakelijk op de betrouwbaarheid van systemen. De methodiek is in de praktijk echter ook uitermate geschikt gebleken om onderzoek te verrichten naar de effectiviteit en de efficiency van informatiesystemen. Het is derhalve van groot belang dat in de beschrijving van de scope wordt vastgelegd aan welke kwaliteitsaspecten aandacht wordt geschonken tijdens het onderzoek.

De opdrachtformulering is gekenmerkt als fase 1 van SRS. Het verdient echter de voorkeur om de opdrachtformulering pas definitief af te ronden nadat met behulp van een vooronderzoek de informatie uit de volgende fase is vergaard. De inzichten in de bedrijfsprocessen en de doelstellingen van de onderneming dragen in belangrijke mate bij tot een betere informatie-uitwisseling met de opdrachtgever over de noodzaak en het belang en daarmee de scope van het onderzoek.

'Understanding the business'

In de fase 'understanding the business' zal de systeembeoordelaar informatie vergaren om inzicht te krijgen in het bedrijf en de markt waarin het opereert. Deze algemene kennis van het bedrijf is noodzakelijk om een beter begrip te krijgen voor het waarom en het belang van het onderzoek en biedt tevens de basis voor het uitvoeren van de risk assessment in de volgende fase. Er moet aandacht worden geschonken aan branche-specifieke kenmerken, de beheersstructuur (management control) van het bedrijf, de bedrijfscultuur, de kritieke succesfactoren en de bedrijfsdoelstellingen.
Een opsomming van de overige aandachtspunten is in figuur 3 weergegeven.

Figuur 3. Overige aandachtspunten bij 'understanding the business'.

- Inzicht in de belangrijkste primaire bedrijfsprocessen
- Inzicht in de belangrijkste informatieverwerkende processen
- Inzicht in de doelstellingen van de te beoordelen processen
- Inzicht in de IT-omgeving
- Inschatting van de mate waarin processen en de beheersing daarvan (management control) afhankelijk zijn van geautomatiseerde systemen ten behoeve van:
  - de beschikbaarheid van informatie;
  - de betrouwbaarheid van informatie;
  - de effectiviteit van informatie;
  - het bewaken van naleving van wet- en regelgeving.

In het kader van de controle van de jaarrekening zal de accountant deze informatie reeds hebben vergaard en kan van deze kennis gebruik worden gemaakt ten behoeve van de systeembeoordeling.

Risk assessment

Uitgaande van de gedefinieerde bedrijfsdoelstellingen in de vorige fase wordt in de fase risk assessment geanalyseerd welke oorzaken (risico's) kunnen bestaan die de realisatie van de doelstellingen bedreigen. Het gaat hierbij uitsluitend om de oorzaken die ertoe leiden dat de informatievoorziening niet betrouwbaar, niet tijdig beschikbaar en/of niet effectief is en die daarmee het systeem van management control en dus de realisatie van de bedrijfsdoelstellingen bedreigen.

Zowel interne als externe factoren kunnen ertoe leiden dat er fouten optreden in de informatievoorziening. De risico's worden in kaart gebracht en er wordt een inschatting gemaakt van de waarschijnlijkheid dat een risico zich voordoet en van de mogelijke impact die het risico heeft op de kwaliteit van de informatievoorziening.

Het gehele proces van risk assessment moet in zeer nauw overleg met de cliënt worden uitgevoerd en de resultaten zullen met het management moeten worden afgestemd alvorens het onderzoek wordt vervolgd. Met deze afstemming wordt in samenwerking met de cliënt uiteindelijk vastgesteld welke risico's in voldoende mate moeten worden beheerst door het te onderzoeken systeem.

Met behulp van de risk assessment kan het onderzoek worden toegesneden op de beheersing van bepaalde risico's. Dit biedt belangrijke efficiencyvoordelen als het management uitsluitend is geïnteresseerd in een beoordeling van de beheersing van specifieke risico's. Het is echter wel belangrijk dat in dat kader de scope van het onderzoek geen geweld wordt aangedaan. Eventuele bijstellingen in de scope moeten nadrukkelijk in de rapportage tot uitdrukking worden gebracht.

In het kader van de controle van de jaarrekening kan de risk assessment eveneens een bijdrage leveren door de beoordeling van de betrouwbaarheid van het systeem toe te spitsen op uitsluitend de kritieke controlerisico's.

'Understanding the target system'

'Understanding the target system' zou het hart van SRS genoemd kunnen worden. In deze fase wordt de noodzakelijke kennis opgebouwd voor het definiëren van de eisen van interne controle in de volgende fase. Het verkrijgen van inzicht in de getroffen maatregelen van interne controle komt bij 'understanding the target system' dus nog niet aan de orde. 'Understanding the target system' leidt

primair tot een helder functioneel inzicht in wat het systeem doet en hoe het systeem dat doet. Het doel van deze fase is dus om een zodanig inzicht te verwerven in het 'target system' dat met behulp van dit inzicht, bij onderkende systeemfuncties en voor de vastgestelde risico's, eisen van interne controle kunnen worden gedefinieerd.

Het proces met behulp waarvan 'understanding the target system' inhoud wordt gegeven, bestaat uit de volgende stappen:
1. procesgewijs onderkennen en analyseren van de gegevensstromen;
2. definiëren van systeemfuncties;
3. verwerken van informatie in een schema met toelichting;
4. verificatie.

Procesgewijs onderkennen en analyseren van de gegevensstromen
Dit is de belangrijkste stap in het doorgronden van het systeem. Bij het analyseren van de gegevensstromen wordt op basis van de uitkomsten van de risk assessment en uit efficiency- en betrouwbaarheidsoverwegingen onderscheid gemaakt tussen:
- wel of niet relevante gegevensstromen;
- kritieke en niet-kritieke gegevens;
- vaste en variabele gegevens.

'Understanding the target system' zou het hart van SRS genoemd kunnen worden.

Uit efficiency-overwegingen wordt een onderscheid gemaakt in gegevensstromen die wel of niet relevant zijn in het kader van de beheersing van de vastgestelde risico's uit fase 3. De gegevensstromen die niet van belang zijn worden verder buiten beschouwing gelaten.

Binnen de wel relevante gegevensstromen wordt met behulp van de uitkomsten van de risk assessment een onderscheid gemaakt tussen kritieke en minder kritieke gegevens. Een gegeven wordt als kritiek aangemerkt indien een fout in dat gegeven één van de gedefinieerde bedrijfsdoelstellingen zal bedreigen. Indien bijvoorbeeld wordt uitgegaan van de bedrijfsdoelstelling 'factureren tegen het juiste kortingspercentage' zullen de naam-, adres- en woonplaatsgegevens van een afnemer niet kritiek zijn en het kortingspercentage van de afnemer wel.

Vervolgens is het belangrijk de gegevensstromen nader te onderscheiden in vaste en variabele gegevens.
Onder vaste gegevens worden de gegevens verstaan die worden gebruikt bij de verwerking van meerdere transacties. Zo is de verkoopprijs die voor de facturering wordt opgehaald uit het artikelenbestand een vast gegeven. Iedere keer als het desbetreffende artikel wordt verkocht, zal diezelfde verkoopprijs worden gebruikt. Dit impliceert dat een fout in een vast gegeven kan leiden tot een lawine van fouten bij de transactieverwerking. Variabele gegevens daarentegen komen veelal maar eenmalig in die hoedanigheid voor en kunnen hooguit leiden tot een fout in één enkele transactie. Zo zal een foutief aan een order toegekende variabele korting leiden tot verkeerde berekening van de korting van uitsluitend die betreffende order.

De gevolgen van fouten in vaste dan wel variabele gegevens zijn dus heel verschillend. Dit heeft invloed op de aard en de 'zwaarte' van de maatregelen die nodig zijn om het risico op fouten in kritieke vaste dan wel variabele gegevens te beheersen. Het maken van onderscheid tussen vast en variabel is dus van belang voor de aard van de te definiëren eisen van interne controle in de volgende fase.

Daarnaast is het van belang om in kaart te brengen wat de bevoegde bedrijfsfuncties zijn. Dit geeft inzicht in de wijze waarop de bevoegdheden binnen het te beoordelen systeem zijn verdeeld. Dit is in een later stadium belangrijk als gekeken wordt naar de getroffen maatregelen zoals functiescheidingen.

De gegevensanalyse vindt per processtap plaats met behulp van het stellen van de volgende twee kernvragen:
1. Waar komt het gegeven vandaan?
2. Wat is de functie van het gegeven in het proces?

Op deze wijze wordt bereikt dat voor alle relevante gegevensstromen het benodigde inzicht wordt verkregen tot op het niveau waarop het niet meer zinvol wordt geacht die vragen te beantwoorden.

De hulpmiddelen die een beoordelaar ter beschikking staan om een goede analyse uit te voeren zijn:
- interviews;
- record-layouts of datamodellen;
- invoerschermen;
- output;
- systeemdocumentatie.

De mix van hulpmiddelen waar een beoordelaar gebruik van maakt, zal in belangrijke mate worden bepaald door zijn achtergrond. Zo zal iemand met een technische achtergrond een goed en snel inzicht kunnen verwerven met behulp van record-layouts, datamodellen en systeembeschrijvingen, terwijl iemand met een functionele achtergrond veel meer houvast zal vinden in de invoerschermen, de output en interviews. SRS is daarin niet dwingend. De beoordelaar moet bij het gebruik van documentatie echter wel aandacht hebben voor het up-to-date zijn daarvan. Belangrijk is dat wordt gekozen voor een zodanige mix van hulpmiddelen dat niet alleen in voldoende mate zekerheid wordt verkregen over de opzet van het systeem maar ook over het bestaan daarvan, indien dit is afgesproken bij de opdrachtformulering.

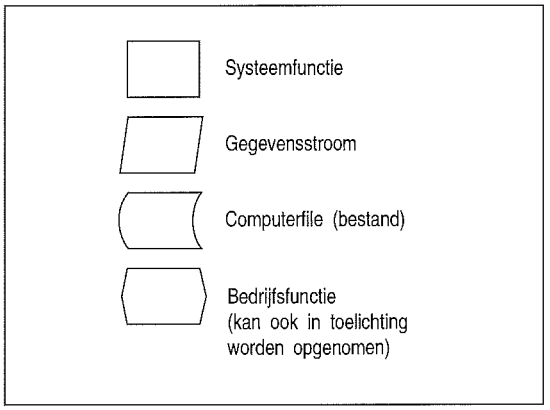
Definiëren van systeemfuncties
In het kader van SRS worden systeemfuncties gedefinieerd als een geheel van logisch bij elkaar behorende gegevensverwerkende activiteiten (automatisch of handmatig). De 'logica' van wat bij

elkaar hoort in deze definitie wordt met name bepaald door het feit dat bij iedere systeemfunctie eenduidige eisen van interne controle moeten kunnen worden gedefinieerd in de volgende fase. De groepering van activiteiten in de systeemfunctie zal daardoor ook aansluiten bij de te beheersen risico's die zijn onderkend in de risk assessment. Het definiëren van de systeemfuncties sluit precies aan op de analyse van de gegevensstromen in de vorige stap. Het niveau waarop systeemfuncties worden onderkend, wordt bepaald door het onderscheid met betrekking tot:
- kritieke vaste gegevens;
- niet-kritieke vaste gegevens;
- kritieke variabele gegevens;
- niet-kritieke variabele gegevens;
- de verantwoordelijke bedrijfsfunctie.

Ook in de aard van de verschillende functies ligt een aanleiding tot verder onderscheid in systeemfuncties. De aard van een functie en daarmee de gevolgen of risico's bij fouten impliceren verschillende beheersmaatregelen, dus dienen in de volgende fase andere eisen van interne controle te worden gedefinieerd. In beginsel zijn er drie functies te onderscheiden:
- bijwerken van gegevensgroepen;
- uitvoeren van beslis- of rekenregels;
- informatieverschaffing.

Verwerken van informatie in een schema met toelichting

Om de functionaliteit van het te onderzoeken (deel van het) systeem duidelijk zichtbaar te maken is in de SRS-methodiek gekozen voor een eenvoudige schematechniek. Omdat het in SRS nadrukkelijk niet gaat om de technische aspecten van de verwerking, is in de praktijk gebleken dat een viertal symbolen voor deze methodiek toereikend is (zie figuur 4).

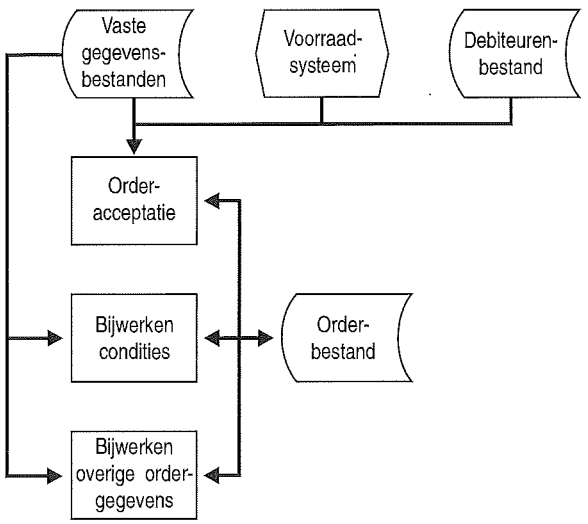


Figuur 4. Symbolen in de schematechniek van SRS.

Het schema en de toelichting geven te zamen inzicht in de gegevensstromen en de systeemfuncties van het te onderzoeken systeem. Teneinde voldoende informatie ter beschikking te hebben voor het definiëren van de eisen van interne controle moet in de toelichting ten minste de volgende informatie worden opgenomen:
- Wat doet de systeemfunctie?
- Welke belangrijke gegevens worden ingevoerd?
- Welke belangrijke gegevens worden overgenomen uit andere bestanden?
- Welke belangrijke gegevens worden uitgevoerd of doorgegeven aan andere bestanden?

Voorbeeld 1. Subschema bijwerken orders.

Subschema Verkoop/Debiteuren/Geldontvangsten-systeem
BIJWERKEN ORDERS



Toelichting

Verantwoordelijke Bedrijfsfunctie:
Verkoop(administratie) in overleg met Financiële administratie.
Bijzondere transacties zijn: contante verkopen, personeelsverkopen en monsters / gratis verzendingen.

Condities betreffen:
- kortingspercentage (variabel);
- facturering in vreemde valuta;
- voorschotfacturering.

Verantwoordelijke Bedrijfsfunctie:
Verkoop(administratie), eventueel in overleg met Financiële administratie.
Invoer: Verkoopadministratie.
Gegevens uit andere bestanden:
- verkoopprijs (Artikelbestand);
- vast kortingspercentage (Klant/artikel-bestand, kan worden overschreven).

Verwerkingstypologie: OL/batch.
Informatieverstrekking: beeldscherm en papier.

Verantwoordelijke Bedrijfsfunctie:
Verkoopadministratie.
Invoer: Verkoopadministratie.
Gegevens uit andere bestanden:
- verzend- en factuuradres (Klantenbestand).

Verwerkingstypologie: OL/batch.
Informatieverstrekking: beeldscherm en papier.

Doss.ref.

- Welke andere relevante informatie levert de systeemfunctie?
- Wat is de verwerkingstypologie?
- Wat is de verantwoordelijke bedrijfsfunctie?
- Wie voert de gegevens in?

Verificatie
In deze stap moeten het schema en de gemaakte toelichting worden afgestemd met de cliënt. Dit is van groot belang omdat op deze wijze misinterpretaties aan de zijde van de beoordelaar nog rechtgezet kunnen worden voordat het onderzoek wordt vervolgd. Verificatie van de door de beoordelaar gemaakte vastlegging is dus absoluut noodzakelijk.

Vaststellen eisen van interne controle op basis van te beheersen risico's

In fase 3 worden de risico's geïnventariseerd die de doelstellingen van de te onderzoeken processen bedreigen en in fase 4 wordt een functioneel inzicht verkregen in de werking van het systeem. Op grond van de opgebouwde kennis over het systeem is het vervolgens noodzakelijk alle gedefinieerde risico's te relateren aan onderkende systeemfuncties, waarna de eisen van interne controle worden gedefinieerd.

Stel dat 'het risico dat te hoge kortingen worden verstrekt' als risico is gedefinieerd. Uit de fase 'understanding the system' is duidelijk geworden dat weliswaar gewerkt wordt met vaste kortingen per klant/per artikel, maar dat deze kortingen onder bepaalde conditie bij de orderentry kunnen worden overschreven.
In dat geval zal 'het risico dat te hoge kortingen worden verstrekt' zowel beheerst moeten worden in de systeemfunctie 'Bijwerken vaste kortingspercentages per klant/per artikel' als in de systeemfunctie 'Bijwerken ordercondities bij orderinvoer'.
Het aldus relateren van de risico's aan de systeemfuncties draagt bij tot het helder definiëren van de eisen van interne controle (zie voorbeeld 2).

Ofschoon de eisen van interne controle inhoudelijk niet van elkaar verschillen, zijn zij gerelateerd aan verschillende systeemfuncties en vragen zij andere maatregelen van interne controle. Let wel: bij het definiëren van de eisen van interne controle gaat het dus niet om het beschrijven van een mogelijke maatregel. Er kunnen namelijk verschillende maatregelen toereikend zijn. Het is dus van belang de eis op een zodanig niveau te definiëren dat de effectiviteit van de feitelijk bij de opdrachtgever geïmplementeerde maatregel daaraan getoetst kan worden.

Op deze wijze ontstaat een normenstelsel van eisen van interne controle waaraan de effectiviteit van de maatregelen van interne controle in de volgende fase kan worden getoetst.

Inventarisatie en evaluatie van beheersmaatregelen

Alvorens de beheersmaatregelen aan de hand van het in de vorige fase gedefinieerde normenkader te kunnen beoordelen op toereikendheid, zullen deze maatregelen eerst per eis van interne controle in kaart moeten worden gebracht. Deze inventarisatie zal voornamelijk geschieden aan de hand van interviews met diverse medewerkers van de cliënt en door directe waarnemingen. Daarnaast kan eventueel gebruik worden gemaakt van documentatie. Van belang is dat naast de interviews aandacht wordt geschonken aan (schriftelijk) bewijsmateriaal en, zoals reeds eerder gesteld bij 'understanding the system', aan afstemming (verificatie) met de cliënt om misinterpretaties te voorkomen.

Bij de evaluatie van de aangetroffen beheersmaatregelen wordt beoordeeld of deze maatregelen toereikend zijn om de gedefinieerde risico's te beheersen. Met andere woorden, wordt er voldaan aan de gestelde eisen van interne controle? Per eis van interne controle zal er sprake zijn van een mix van beheersmaatregelen. Deze mix is dan ook het object van beoordeling.

Maatregelen van interne controle kunnen preventief dan wel repressief van aard zijn. Bij preventieve controles moet gedacht worden aan geprogrammeerde controles en de algemene computercontroles. Repressieve controles vinden achteraf plaats en zijn veelal handmatige gebruikerscontroles. Bij de beoordeling van de effectiviteit van een beheersmaatregel moet rekening worden gehouden met de aard van de maatregel, de eis die aan de maatregel wordt gesteld en de verwerkingstypologie (zoals batch of realtime). Een postorderbedrijf dat binnen vierentwintig uur levert, kent bijvoorbeeld een groot belang toe aan de juistheid van de orderinvoer (die online/realtime wordt ingevoerd en verwerkt). Indien de orderinvoer niet juist is zal dit leiden tot verkeerde leveringen welke gecorrigeerd moeten worden, hetgeen onnodige kosten zal veroorzaken. Gezien de verwerkingstypologie en het feit dat binnen vierentwintig uur wordt geleverd, zal gebruik moeten worden gemaakt van preventieve maatregelen zoals geprogrammeerde invoercontroles. Repressieve gebruikerscontroles komen in dit verband te laat en dienen dan ook te worden beoordeeld als niet effectief.

Op basis van de risk assessment is vastgesteld wat kritieke dan wel niet-kritieke gegevens zijn. Of er sprake is van een al dan niet kritiek vast of variabel gegeven heeft invloed op de gestelde eisen van interne controle, hetgeen daardoor ook invloed

Voorbeeld 2. Relatie systeemfuncties en eisen van interne controle.

Systeemfunctie	*Eis van interne controle*
Bijwerken vaste kortingspercentages per klant/per artikel (online/batch).	Hoge mate van zekerheid over de juistheid en autorisatie van de ingevoerde vaste kortingen.
Bijwerken ordercondities bij orderinvoer (online/batch).	Hoge mate van zekerheid over de juistheid en autorisatie van de ingevoerde variabele kortingen.

heeft op de beoordeling van de toereikendheid van de getroffen beheersmaatregelen.

Inhakend op voorbeeld 2 van de vaste en variabele kortingspercentages uit de vorige fase zou het inventariseren en evalueren van aangetroffen beheersmaatregelen per eis van interne controle kunnen worden vastgelegd als weergegeven in voorbeeld 3.

De output van deze fase bestaat dus uit een vastlegging van alle aangetroffen beheersmaatregelen per eis van interne controle 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.

Eis van interne controle	*Aangetroffen maatregelen en beoordeling*
Hoge mate van zekerheid over de juistheid en de autorisatie van de ingevoerde vaste kortingen.	Integrale controle achteraf met behulp van een doorlopend genummerd mutatieverslag en het invoerdocument door een andere functionaris dan degene die de mutatie heeft ingevoerd. Verslag naar hogere functionaris. *Akkoord* Autorisatie door hoofd Verkoop en Directie. *Akkoord*
Hoge mate van zekerheid over de juistheid en de autorisatie van de ingevoerde variabele kortingen.	Geprogrammeerde controle op de acceptatie van de kortingen binnen door de Directie vastgestelde marges. Afwijkingen worden wel geaccepteerd door het systeem en achteraf door het hoofd Verkoop geautoriseerd met behulp van signaleringslijst. *Akkoord*

Voorbeeld 3. Beheersmaatregelen per eis van interne controle.

Rapportage

Bij de opdrachtformulering is reeds aangegeven in welke vorm de onderzoeksresultaten worden gerapporteerd aan de opdrachtgevers. Van belang is dat de gekozen vorm van de rapportage aansluit bij de verwachtingen van de cliënt. De rapportage moet zorgen dat de nodige aandacht en follow-up van de zijde van de ontvangende partij wordt verkregen. Hiertoe dient de rapportage beknopt en doeltreffend te zijn. Het 'succes' van de systeembeoordeling in de ogen van de opdrachtgevers is sterk afhankelijk van de rapportage. Het behoeft ons inziens daarom geen betoog dat de nodige zorg aan deze laatste fase dient te worden besteed.

Voorwaarden voor een goede rapportage zijn onder meer:
- een duidelijke opdrachtformulering;
- een goed opgezet en uitgevoerd onderzoek;
- de medewerking van en feedback aan het betrokken management.

Naast deze voorwaarden bestaat ook een aantal middelen om tot goede rapportage te komen. Hierbij kan gedacht worden aan het gebruik maken van een standaard-rapportindeling, het scheiden van hoofd- en bijzaken, het vermijden van vakjargon en afkortingen, zorgen voor een duidelijke samenhang en het voorbespreken van de onderzoeksresultaten met het management. In het rapport dienen de conclusie en de samenvatting van de voornaamste bevindingen en aanbevelingen ten behoeve van het hoger management te worden uitgewerkt. De verdere detailleringen, zoals de uitkomsten per fase, kunnen in de bijlagen worden ondergebracht.

TOEPASBAARHEID SRS

SRS is een systeembeoordelingsmethodiek die niet alleen toepasbaar is op systemen die reeds in gebruik zijn, maar ook op systemen in ontwikkeling. In dat geval zal gebruik worden gemaakt van bijvoorbeeld functionele specificaties en prototypes om voldoende inzicht te krijgen in het te beoordelen systeem.

Daarnaast blijkt SRS een uitstekend produkt om in te zetten bij de controle van de jaarrekening teneinde de voldoende inzicht te krijgen in de belangrijke

- Vaststelling controlestrategie
- Planning controle
- Verkrijgen effectief controlebewijs
- Afsluitende beoordeling en evaluatie van controlebevindingen
- Rapportering
- Slotevaluatie

systemen en de daarin getroffen maatregelen van interne controle.
Indien de fasen van SRS naast de fasering van het controleproces ([Munc95]) worden gelegd, blijkt dat er grote overeenkomsten bestaan.
Figuur 5. Fasering van het controleproces.

Bij het vaststellen van de controlestrategie zal de accountant inzicht verwerven in het bedrijf van de cliënt, vaststellen welke bedrijfsrisico's en -doelstellingen van toepassing zijn en het daaraan gerelateerde beheersconcept van de onderneming in grote lijnen in kaart brengen. Bij SRS komt dit overeen met de fasen 'understanding the business' en risk assessment. In de planning van de controle stelt de accountant de belangrijkste controledoelstellingen vast. Ook zal de accountant in deze fase het beheersconcept van de onderneming (de AO/IC) beschrijven en beoordelen. Deze werkzaamheden zijn vergelijkbaar met de volgende drie fasen van SRS, namelijk 'understanding the target system', het vaststellen van de eisen van interne controle op basis van te beheersen risico's en de inventarisatie en evaluatie van beheersmaatregelen.

SRS richt zich op de opzet en het bestaan van het systeem en de bijbehorende beheersmaatregelen.

Mw. drs. M.J.A. Koedijk RA
Is sinds 1991 werkzaam in de controlepraktijk bij KPMG. Sinds 1 april 1995 is zij werkzaam als supervisor bij KPMG EDP Auditors maar is daarbij deeltijds werkzaam gebleven in de controlepraktijk. Zij heeft na een doctorale opleiding Bestuurlijke Informatiekunde in 1995 de postdoctorale opleiding Accountancy afgerond.
Zij is actief in de ontwikkeling van methoden, produkten en trainingen die bijdragen tot het verbeteren van de samenwerking tussen accountants en EDP-auditors ten behoeve van de jaarrekeningcontrole.
Zij voert systeembeoordelingen volgens de SRS-methodiek uit en treedt op als docent van interne en externe cursussen.

Mw. W.A. de Munck RA
Is werkzaam als senior manager bij KPMG EDP Auditors en richt haar aandacht voornamelijk op EDP-auditwerkzaamheden in het kader van de controle van de jaarrekening. Zij is mede verantwoordelijk voor het ontwikkelen van methoden, produkten en trainingen die bijdragen tot het verbeteren van de samenwerking tussen accountants en EDP-auditors ten behoeve van de jaarrekeningcontrole.
Zij geeft leiding aan SRS-onderzoeken, onder meer in het kader van de jaarrekeningcontrole.

Deze opzet en het bestaan van het beheersconcept wordt gerelateerd aan de onderkende risico's respectievelijk controledoelstellingen en vervolgens beoordeeld. Het verkrijgen van een effectief controlebewijs wordt niet uitgewerkt in SRS. De accountant zal door middel van systeemtests inzicht moeten krijgen in de werking van het systeem. Een EDP-auditor kan hierbij de accountant ondersteunen, mede omdat een deel van de zekerheid omtrent de werking van geprogrammeerde controles kan worden ontleend aan de goede werking van de algemene beheersmaatregelen, zoals reeds eerder in dit artikel werd gesteld.

CONCLUSIE

Samenvattend kan worden geconcludeerd dat SRS de mogelijkheid biedt om op efficiënte wijze met behulp van een inventarisatie van de risico's die de doelstellingen van bedrijfsprocessen bedreigen, de betrouwbaarheid van informatiesystemen te beoordelen. Op basis van een procesgerichte benadering wordt voldoende inzicht verkregen in de functionaliteit van het systeem en de wijze waarop het systeem het management control van de bedrijfsprocessen ondersteunt, en kunnen heldere eisen van interne controle worden gesteld aan het informatiesysteem. Deze eisen dienen als basis om de effectiviteit van getroffen (of te treffen) maatregelen van interne controle eenvoudig te kunnen beoordelen.
SRS volgt een sterk functionele benadering, hetgeen als belangrijk voordeel biedt dat het onderzoek ook grotendeels kan worden uitgevoerd door beoordelaars met een minder sterke technische achtergrond. Het is derhalve een krachtig hulpmiddel dat ook in het kader van de controle van de jaarrekening een vaste plaats verdient.

LITERATUUR

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

[KPMG95] Interne (internationale) documentatie omtrent de SRS-methodiek.

De EDP-auditor: vertrouwensman, agent of ...?

Drs. H.E. Sijbring RE RA

Het beroep van EDP-auditor heeft een veel kortere bestaansgeschiedenis dan het accountantsberoep. Door deze kortere geschiedenis is de relatie tussen de EDP-auditor en het maatschappelijk verkeer minder uitgekristalliseerd in vergelijking met de accountant.
De auteur beschrijft in hoeverre op het beroep van EDP-auditor dezelfde grondslagen van toepassing zijn als op het beroep van accountant. Hij geeft aan in welke mate een aantal theorieën, die deels ontleend zijn aan de accountancy, als fundament kunnen dienen voor het bestaansrecht van het accountantsberoep en op basis van deze bevindingen voor het bestaansrecht van het beroep van EDP-auditor.

INLEIDING

Al sinds de dertiger jaren, toen Limperg zijn Leer van het Gewekte Vertrouwen formuleerde, ontleent de Nederlandse openbare accountant zijn functie aan zijn maatschappelijke rol. De behoefte aan een getrouwheidsoordeel bij de jaarverslaggeving van ondernemingen heeft de accountantsfunctie vorm gegeven.

Waar Limperg een soort voortdurende vertrouwensrelatie veronderstelde tussen de accountant en het maatschappelijk verkeer, bleek in praktijk een fikse kloof te ontstaan tussen datgene wat de samenleving verwacht van de accountant, en datgene wat de accountant de samenleving in feite biedt. Hoe heeft het zover kunnen komen? Hoe is deze verwachtingskloof ontstaan? In de literatuur is de oplossing deels gezocht in het definiëren van een andere grondslag voor het accountantsberoep, namelijk de Agency-theorie.

Een veel kortere bestaansgeschiedenis heeft het beroep van EDP-auditor. Hierdoor is de relatie tussen de EDP-auditor en het maatschappelijk verkeer nog niet (geheel) uitgekristalliseerd. Is het mogelijk dat de EDP-auditor te maken krijgt of reeds heeft met dezelfde verwachtingskloof als de accountant? Fungeert de EDP-auditor als 'vertrouwensman van het maatschappelijk verkeer' (conform de Vertrouwenstheorie van Limperg), als 'agent' (conform de Agency-theorie) of is hij zowel agent als vertrouwensman?

In de opleiding tot Registeraccountant wordt veel aandacht geschonken aan de grondslagen van het beroep, te weten Vertrouwens- en Agency-theorie. De 'Management Control'-benadering staat centraal in de post-doctorale opleiding tot Register EDP-auditor aan de Erasmus Universiteit Rotterdam (EUR). In dit artikel zal worden onderzocht of op het beroep van EDP-auditor dezelfde grondslagen van toepassing zijn als op het beroep van accountant en in hoeverre de 'Management Control'-benadering nieuwe elementen toevoegt aan de grondslagen van het beroep van EDP-auditor.

Eerst worden de beide grondslagen van de accountantsfunctie beschreven: de Vertrouwenstheorie van Limperg en de Agency-theorie. Vervolgens wordt nagegaan in hoeverre de functie van EDP-auditor te herleiden is op deze grondslagen. Ten slotte wordt de relatie met de 'Management Control'-benadering besproken. Afsluitend worden de samenvatting en de conclusies gegeven.

De in dit artikel besproken problematiek beperkt zich tot de vergelijking van de grondslagen van de accountant en de EDP-auditor die optreden in het maatschappelijk verkeer. Dit kan zowel de opdrachtgever zijn als degene die gebruik maakt van de produkten opgeleverd door de accountant/EDP-auditor. Het doel van dit artikel is het leveren van een bijdrage aan de vaktechnische onderbouwing van het vakgebied EDP-auditing.

HET ONTSTAAN VAN DE BEROEPEN VAN ACCOUNTANT EN EDP-AUDITOR

Het accountantsberoep wordt door de meeste mensen ingedeeld in de categorie jonge beroepen. Het is inderdaad waar, dat de accountant niet kan wijzen op geschiedbronnen die tot in de klassieke oudheid teruggaan. Toch is de accountant al vlot opgedoken in de historie van de ondernemende mens. De plicht zich te verantwoorden, als gevolg van de scheiding tussen eigendom en beheer van vermogensbestanddelen, deed de behoefte ontstaan aan een oordeel over de betrouwbaarheid van die verantwoording.
De bestudering van de geschiedenis van het accountantsberoep in Nederland voert ons terug naar het eind van de negentiende eeuw. In 1883 werd in Rotterdam het boekhoudkundig bureel 'Confidentia' opgericht. De oprichters van dit bureau waren een aantal jaren later, in 1895, medeinitiatiefnemers tot de oprichting van NIVA, het Nederlands Instituut Voor Accountants. Deze periode is het begin geweest van het vormingsproces van het zelfstandige Nederlandse accountantsberoep.

Het ontstaan van een zelfstandige beroepsgroep leidt tot het ontstaan van een verwachtingspatroon bij het maatschappelijk verkeer.

Een veel kortere bestaansgeschiedenis heeft het beroep van EDP-auditor. Omstreeks 1950 doet de automatisering haar intrede. Vanaf begin jaren zestig worden mainframes algemeen ingezet, vanaf 1975 gevolgd door de minicomputer. Vanaf 1985 wordt de personal computer op grote schaal ingevoerd en computernetwerken volgen vanaf midden negentiger jaren. Dit gebruik heeft geleid tot een grote afhankelijkheid van de automatisering. De complexiteit van de automatisering neemt sterk toe evenals de investeringen in en de kosten van het in stand houden van de automatisering. Automatisering heeft geleid tot het ontstaan van de vierde produktiefactor 'informatie'. Gesteld kan worden dat de kwaliteit van de informatievoorziening veelal bepalend is voor een succesvol functioneren van organisaties. Organisaties worden zich steeds meer bewust van de noodzaak van het adequaat beheersen van de automatisering, beter gezegd van de informatievoorziening.

Voor het uitvoeren van de jaarrekeningcontrole stelt de accountant vast welke controlewerkzaamheden hij moet uitvoeren om tot zijn oordeel te kunnen komen. Hierbij kan of moet hij in bepaalde mate steunen op interne-controlemaatregelen die binnen de organisatie zijn getroffen. Met de intrede van de automatisering heeft er binnen organisaties veelal een verschuiving plaatsgevonden van de wijze waarop interne-controlemaatregelen zijn uitgevoerd. Gebruikerscontroles zijn vervangen door interne-controlemaatregelen die met behulp van de automatisering zijn gerealiseerd (bijvoorbeeld geprogrammeerde controles en logische toegangsbeveiliging) en de automatisering vormt ook zelf een object van interne controle. Steeds vaker kan de accountant voor het vormen van een oordeel over de getrouwheid van de jaarrekening niet meer 'om de computer heen' controleren.

In eerste instantie schakelden de organisaties hun accountant in bij het vormen van een oordeel over de kwaliteit van de automatisering en kon deze dit er 'vaktechnisch' nog wel bij doen. Ook kon de accountant voor het oordeel over de automatisering in het kader van de jaarrekeningcontrole het zelf nog wel aan. Maar de sterke toename van het aantal jaarrekeningcontroles waarbij de accountant steunt op de automatisering en het aantal opdrachten waarbij het management als opdrachtgever optreedt, heeft hierin verandering gebracht. De vereiste beschikking over specialistische kennis en ervaring, nodig voor een succesvolle uitvoering van deze opdrachten, heeft geleid tot de ontwikkeling van een eigen beroepsgroep: de EDP-auditors.

Het ontstaan van een zelfstandige beroepsgroep leidt tot het ontstaan van een verwachtingspatroon bij het maatschappelijk verkeer. Evenzo is een beroep onderworpen aan de invloed van de samenleving. Een voorbeeld uit een ander vrij beroep is wellicht illustratief: verwijsbriefjes van artsen gaan tegenwoordig, onder druk van een steeds mondiger wordende patiënt, niet meer in hermetisch gesloten enveloppen. De beroepsgroep dient altijd oog te hebben voor wijzigingen in de economische en maatschappelijke omstandigheden die invloed uitoefenen op de feitelijke inhoud van de functie en het beroep.

LIMPERG EN DE VERTROUWENSTHEORIE

Uitleg Vertrouwenstheorie

De beroepsopvattingen van de accountants in Nederland steunen (nog steeds) sterk op de Vertrouwenstheorie van Limperg. Tijdens het Internationale Accountantscongres te Amsterdam in 1926 heeft Limperg in een artikel de grondslag gelegd voor de taak, functie en verantwoordelijkheid van de accountant. Dit artikel heeft hij later uitgewerkt in een viertal artikelen, die in 1932 en 1933 gepubliceerd zijn in het Maandblad voor Accountancy en Bedrijfshuishoudkunde ([Limp32,33]). De artikelenreeks is overigens een soort 'Unvollendete', omdat het expliciete '(slot volgt)' aan het einde van het vierde artikel nooit heeft geresulteerd in een daadwerkelijk slot. Dat dit niets afdoet aan de waarde van de artikelen voor het beroep behoeft mijns inziens geen betoog.

Limperg onderscheidt in zijn visie, aangeduid als De Leer van het Gewekte Vertrouwen, de volgende kernvraagstukken: de functie van de accountant, de taakinhoud van de accountant en de factoren die de taakinhoud bepalen.

De functie van de accountant is die van controleur/adviseur van de bedrijfsleiding en van het maatschappelijk verkeer. Het maatschappelijk verkeer eist in ruil voor de beschikbaarstelling van financieringsmiddelen verantwoording over het gevoerde beleid. Een oordeel over die verantwoording kan in een steeds gecompliceerder bedrijfsleven slechts gegeven worden door een onafhankelijk controledeskundige: de accountant. De accountant doet zijn intrede in de maatschappij als vertrouwensman van het maatschappelijk verkeer, volgens Limperg de hoofdfunctie van de accountant.

De taakinhoud van de accountant wordt bepaald door de rationele eisen die de functie stelt. Iets minder cryptisch geformuleerd komt het erop neer dat de accountant die arbeid moet verrichten, die nodig is om het in hem gestelde vertrouwen te rechtvaardigen. Aan de andere kant mag er geen groter vertrouwen in de functievervulling van de accountant worden gesteld, dan gerechtvaardigd wordt door zijn verrichte werkzaamheden en zijn deskundigheid.
Er zijn dus twee risico's:
- de accountant kan zijn taak onvoldoende vervuld hebben;
- het maatschappelijk verkeer kan een te hoge verwachting hebben van het werk van de accountant.

Dit laatste risico doet Limperg als volgt af: 'Het maatschappelijk verkeer is verstandig en redelijk, het stelt zijn norm van vertrouwen niet hoger dan de bekwame en zorgvuldig arbeidende accountant vermag te bevredigen'. Het is deze norm, die volgens de leer van het gewekte vertrouwen de inhoud van dat vertrouwen bepaalt ([Limp32,33]). Een overdreven vertrouwen bij het maatschappelijk verkeer is volgens Limperg het gevolg van ondeskundigheid van de accountant: het gaat om het vertrouwen dat de accountant heeft gewekt bij de verstandige leek.
Aldus bestempelt Limperg het vaktechnisch instrumentarium van de accountant als het enige criterium dat van invloed mag zijn op de omvang van de controle en de te bereiken graad van zekerheid.

Eén van de kernbegrippen uit het gedachtengoed van Limperg is de verstandige leek, als simplificatie van dat deel van het maatschappelijk verkeer waar de accountant als vertrouwensman mee te maken heeft. Om het theoretische concept van de verstandige leek te kunnen plaatsen, is het essentieel de leek te plaatsen in de tijd waarin Limperg zijn ideeën heeft ontvouwd.

In het tijdvak tussen de twee wereldoorlogen overheerste het volgende beeld van de onderneming: een zelfstandige eenheid, ontstaan door de scheiding van leiding en eigendom. Omdat men uitging van een stabiele economische buitenwereld, was de onderneming nog een gesloten model. Limperg heeft het in het eerste van zijn artikelen over de verschillende vormen van financiering waarmee de moderne ondernemer te maken heeft. Later geeft hij aan dat het maatschappelijk verkeer verantwoording eist over het beheer van de door hem toevertrouwde spaarpenningen. Het lijkt dus dat Limperg de verstandige leek in slechts één bepaalde hoedanigheid ziet, namelijk die van vermogensverschaffer! In die tijd was dat natuurlijk niet vreemd, omdat er niet veel andere belanghebbenden bij de verslaggeving van de ondernemingen waren.

Het beeld van de onderneming is na 1945, onder invloed van de economische, sociale en technologische ontwikkelingen, omgevormd tot een open model. De onderneming wordt in dit open model wel beschouwd als een subsysteem van het grote maatschappelijke systeem. Als gevolg daarvan bestaat de onderneming nu uit een netwerk van participanten, die allen een bepaalde relatie met de onderneming hebben. Dit proces wordt ook wel de vermaatschappelijking van de onderneming genoemd.

Het maatschappelijk verkeer kan een te hoge verwachting hebben van het werk van de accountant.

Tegelijkertijd speelt zich een proces af, dat alle accountants betreft: de ontsokkeling van het vrije beroep. Hieronder wordt een maatschappelijke en sociale trend verstaan die, globaal genomen, hooggeplaatsten van hun voetstuk haalt. Als gevolg van de toename van de mondigheid, een hoger opleidingsniveau, een groter aantal mensen dat deelneemt aan de informatieverstrekking en het feit dat vroeger onopgemerkte schandalen nu in de openbaarheid komen, kalft het van oudsher als vanzelfsprekend aangenomen gezag van de accountant langzaam af. Er is geen plaats meer voor blind vertrouwen in een beroepsgroep die een produkt aflevert dat maar heel moeilijk op toegevoegde waarde getoetst kan worden. Dit proces overkomt alle beoefenaren van vrije beroepen. En waar autoriteit wegvalt, moet authenticiteit zichzelf bewijzen. Er is een discrepantie ontstaan tussen datgene wat een samenleving verwacht van de accountant, en datgene wat de accountant in feite biedt, of vanuit zijn beroepsopvattingen pretendeert te bieden. Dit verschijnsel wordt aangeduid met de term *verwachtingskloof.*

De waarde van de Vertrouwenstheorie voor de accountant als beroepsgrondslag in deze tijd

Zoals reeds in de vorige subparagraaf is aangegeven, steunen de beroepsopvattingen van de accountants in Nederland sterk op de Vertrouwenstheorie van Limperg. Er dient te worden geconcludeerd dat de Vertrouwenstheorie van Limperg in deze tijd niet meer kan gelden als *het* fundament van het accountantsberoep. Eigenlijk geeft het loutere bestaan van de verwachtingskloof dit al aan, omdat de verwachtingskloof in het theoretisch concept van Limperg per definitie niet voor kan komen. Voor het overbruggen van de verwachtingskloof tussen accountants aan de ene kant en

de samenleving aan de andere kant, dient in ieder geval te worden afgestapt van de termen 'verstandige leek' en 'maatschappelijk verkeer' zoals gedefinieerd door Limperg. Door de in de vorige subparagraaf beschreven maatschappelijke ontwikkelingen kan niet meer worden volstaan met deze ongedifferentieerde termen. Het maatschappelijk verkeer bestaat niet alleen meer uit aandeelhouders maar bijvoorbeeld ook uit leveranciers, afnemers, werknemers, concurrenten, banken en de overheid.

Het maatschappelijk verkeer meet zijn verwachtingen af aan de uitkomsten van de door de accountant uitgevoerde werkzaamheden. Deze uitkomsten zijn vastgelegd in de verklaring van de accountant aan het maatschappelijk verkeer. Het grootste deel van de werkzaamheden van de accountant heeft altijd bestaan uit het beoordelen van de getrouwheid van een financiële verantwoording, veelal de jaarrekening. De uitkomsten van zijn beoordeling zijn vastgelegd in de accountantsverklaring. Bij de formulering van deze verklaring is de accountant altijd uitgegaan van de ongedifferentieerde termen 'verstandige leek' en 'maatschappelijk verkeer'.

Het NIVRA heeft omstreeks 1990 wijzigingen aangebracht in de systematiek en de formuleringen van de accountantsverklaringen teneinde een effectievere communicatie met de doelgroep van deze verklaringen te realiseren. In deze verklaringen wordt met name een nadere omschrijving opgenomen van de normen die de accountant heeft gehanteerd. De omschrijving bestaat uit een verwijzing naar algemeen aanvaarde grondslagen en wettelijke normen (Titel 9 Boek 2 BW).
Echter, deze wijzigingen hebben niet geleid tot het opnemen van een verwijzing naar of een omschrijving van het deel van het maatschappelijk verkeer waarvoor de verklaring is bestemd.

In 1991 heeft het NIVRA registeraccountants de mogelijkheid gegeven om bij zogenaamde controleverwante opdrachten accountantsverklaringen te verstrekken. Redenen hiervoor zijn geweest het behouden van aansluiting op internationale ontwikkelingen en tegemoet komen aan de vraag van delen van het maatschappelijk verkeer naar oordelen van de accountant met een lagere zekerheid van de getrouwheid van de jaarrekening.
Het NIVRA stelt in de 'Richtlijnen voor de Accountantscontrole nummer 001' het volgende: 'De inschakeling van de accountant bij (financiële) informatie wekt vertrouwen op bij de gebruikers van deze informatie. De accountant voegt op grond van zijn werkzaamheden geloofwaardigheid toe, of, anders gezegd hij verschaft een bepaalde mate van zekerheid aan de gebruikers met betrekking tot de betrouwbaarheid van de informatie. De mate van verschafte zekerheid is afhankelijk van de aard en de omvang van de werkzaamheden welke de accountant verricht. Teneinde de verschillende niveaus van te verschaffen zekerheid duidelijk ten opzichte van elkaar af te bakenen ..... wordt een onderscheid gemaakt tussen controle- en controleverwante opdrachten' ([NIVR1]).
Begin oktober 1995 hebben de leden van het NIVRA ter beoordeling een voorstel van het NIVRA ontvangen voor de nieuwe teksten voor de beoordelings- en samenstellingsverklaringen ([NIVR2]). In deze teksten is wederom geen enkele verwijzing of omschrijving opgenomen van de doelgroep waarvoor de verklaring is bestemd.

Uit het bovenstaande kan worden afgeleid dat het NIVRA nog steeds uitgaat van de ongedifferentieerde termen 'verstandige leek' en 'maatschappelijk verkeer', althans in ieder geval die indruk wekt door de gekozen formulering van de diverse soorten accountantsverklaringen. Des te langer het begrippenpaar 'verstandige leek' en 'maatschappelijk verkeer' nog wordt gebruikt zoals die destijds zijn gedefinieerd door Limperg, des te verder zullen de accountant en de afnemers van zijn diensten uit elkaar groeien. Er wordt dan niet voldoende recht gedaan aan het gecompliceerde web van relaties, waarbinnen een organisatie functioneert.

De Vertrouwenstheorie kan nog steeds een fundament vormen van het beroep van accountants indien de accountant zichzelf niet beschouwt als de vertrouwensman van het gehele maatschappelijk verkeer, maar als de vertrouwensman van *een deel van* het maatschappelijk verkeer.
Het begrip 'verstandige leek' dient overboord te worden gezet, aangezien is geconcludeerd dat in deze tijd niet gesproken kan worden van een maatschappelijk verkeer als homogene eenheid. Het huidige maatschappelijk verkeer bestaat uit een heterogeen samenstel van individuen en organisaties. Elk individu en elke organisatie heeft zijn eigen opvattingen en verwachtingen over de functie van de accountant. Het begrip 'maatschappelijk verkeer' kan wel worden gebruikt mits de volgende definitie wordt gehanteerd: 'het heterogene samenstel van individuen en organisaties dat invloed uitoefent op en/of gebruik maakt van de diensten van de accountant'.

De waarde van de Vertrouwenstheorie als fundament voor de EDP-auditor

In de subparagraaf Uitleg Vertrouwenstheorie is aangegeven dat degenen die verantwoordelijk zijn voor het nemen van de automatiseringsbeslissingen en andere belanghebbenden op een of andere manier moeite hebben met het beoordelen van de automatisering en daarvoor als deskundige de EDP-auditor inschakelen. Nog sterker dan de accountant heeft de EDP-auditor te maken met een gecompliceerd web van relaties waarbinnen hij zich moet bewegen. De grote verscheidenheid aan opdrachten, het ontbreken van gestandaardiseerde rapportagevormen binnen de beroepsgroep en het grote aantal verschillende soorten afnemers van zijn diensten zijn hiervan mede de oorzaak.

De Vertrouwenstheorie van Limperg kan alleen een fundament vormen voor het beroep van EDP-auditor mits overeenkomstig hetgeen is gezegd voor de accountant het begrip 'verstandige leek' overboord is gezet en het maatschappelijk verkeer wordt gezien als een heterogeen samenstel van individuen en organisaties, waarbij elk individu en elke organisatie zijn eigen opvattingen en verwachtingen over de functie van de EDP-auditor heeft.

De EDP-auditor dient het begrip 'maatschappelijk verkeer' als volgt te definiëren: 'het heterogene samenstel van individuen en organisaties dat invloed uitoefent op en/of gebruik maakt van de diensten van de EDP-auditor'.

In de volgende paragraaf zal een bedrijfseconomische invalshoek worden gekozen teneinde na te gaan of er nog een fundament te vinden is voor het bestaansrecht van het beroep van EDP-auditor. Gekeken zal worden in hoeverre de Agency-theorie een tweede fundament kan vormen.

AGENCY-THEORIE

Uitleg Agency-theorie

Aan het einde van de jaren zeventig ontstond er een nieuwe stroming in de economische theorie. De nieuwe theorie die hieruit voortvloeide is te beschouwen als een economische organisatietheorie en wordt aangeduid met de naam Agency-theorie.

Centraal in de Agency-theorie staat de contractuele relatie tussen een opdrachtgever, de principaal, en de opdrachtnemer, de agent. In het contract geeft de principaal de agent de opdracht iets voor hem te doen. Voor het uitvoeren van het contract ontvangt de agent een vooraf vastgestelde beloning. Dit contract kan een formele (juridische) status hebben, maar dat hoeft niet. Ook allerlei afspraken die bijvoorbeeld worden gemaakt in het kader van een werkoverleg binnen een organisatie vallen onder het begrip contract.

De agent wordt belast met de opdracht, omdat hij om allerlei redenen hiervoor beter uitgerust is dan de principaal. De principaal is niet altijd in staat het inspanningsniveau van de agent te meten, waardoor hij min of meer afhankelijk wordt van de agent en daardoor aangewezen is op de berichtgeving van de agent.

De relatie tussen principaal en agent wordt agency-relatie genoemd. Agency-relaties komen vaak voor. Bekende voorbeelden zijn:

- de relatie tussen manager en aandeelhouder. De aandeelhouders stellen een groep managers aan om het bedrijf op een verantwoorde manier te leiden en daarmee de waarde van het aandeel te maximaliseren;
- de relatie tussen patiënt en arts. De patiënt verlangt van de arts dat de arts een passende geneeswijze voorschrijft. De arts fungeert als agent en de patiënt als principaal.

Het is plausibel te veronderstellen dat de agent niet altijd zijn werk zal verrichten in volkomen overeenstemming met de belangen van de principaal. Dit probleem wordt het agency-probleem genoemd. In het geval van de manager en de aandeelhouder is het denkbaar dat de manager geldmiddelen van het bedrijf aanwendt om zichzelf te bevoordelen met overbodige zakenreizen en te luxueuze kantoren. In de relatie tussen arts en patiënt is de kans aanwezig dat de arts bij het voorschrijven van zekere geneesmiddelen belangen heeft die niet overeenkomen met de lichamelijke, geestelijke en financiële belangen van de patiënt. Te denken valt aan de royale stroom aan relatiegeschenken van de farmaceutische industrie richting arts ter bevordering van het voorschrijven van bepaalde middelen.

Het ontstaan van het agency-probleem is te wijten aan belangendivergentie.

Het ontstaan van het agency-probleem is te wijten aan belangendivergentie. De Agency-theorie hanteert als veronderstelling dat de agent in eerste instantie voor zijn eigen belangen zal kiezen. Zonder afdoende prikkels zal hij zich opportunistisch opstellen tegenover de principaal. Bij alle beslissingen die de agent neemt zal hij zich elke keer afvragen: 'Zal ik mijn belang voor het belang van de principaal laten prevaleren?'
De principaal weet dat hij te maken heeft met deze belangendivergentie en zal daarom kosten maken om deze belangendivergentie zo goed mogelijk in kaart te brengen en, waar mogelijk, te reduceren. Ook de agent heeft uit kostenoogpunt vaak belang bij het verkleinen van deze belangendivergentie en zal daardoor bepaalde kosten maken. De kosten van zowel de principaal als de agent worden de agency-kosten genoemd. De agency-kosten bestaan uit de volgende componenten:

Monitoring costs
Dit zijn kosten die de principaal maakt om zijn agent te controleren op naleving van het contract.
Een voorbeeld: de kosten van een controleur die, in dienst van een winkelbedrijf, de kwaliteit van de ingekochte levensmiddelen vaststelt, en toetst aan het inkoopcontract.

Bonding costs
Dit zijn kosten die de agent maakt om de principaal duidelijk te maken dat hij zich aan de contractuele verplichtingen houdt.
Een voorbeeld: de kosten die de verkoper van brandstoffen maakt om zijn pompen te laten voorzien van een keurmerk van het ijkwezen.

Residual loss
Dit zijn de restkosten die het gevolg zijn van beslissingen die een agent neemt, en die niet tot een optimaal resultaat leiden, althans niet vanuit de optiek van de principaal.
Een voorbeeld: de kosten voor het afgraven van vervuilde grond onder een voormalig industrieterrein.

De aard van de kostenpost is niet zonder meer bepalend voor het feit of een uitgave wordt aangemerkt als monitoring of bonding; het gaat om de vraag welke contractpartner voor welk doel kosten maakt. Het kan dus heel goed zijn, dat een bepaalde uitgave in het ene geval een monitoring-cost is

en in het andere geval een bonding cost. In het gegeven voorbeeld van het ijkwezen zou een bonding-karakter van de kostenpost veranderen in een monitoring-karakter, als de afnemers van de brandstoffen de pompen op hun kosten zouden laten ijken.

De accountant in de Agency-theorie

In de paragraaf over de Vertrouwenstheorie is aangegeven dat de plicht zich te verantwoorden, als gevolg van de scheiding tussen eigendom en beheer van vermogensbestanddelen, de behoefte deed ontstaan aan een oordeel over de betrouwbaarheid van die verantwoording. De principalen van de ondernemingsleiding kunnen te maken krijgen met problemen die voortvloeien uit de contractrelatie. Zo kunnen aandeelhouders benadeeld worden door buitensporige kostenconsumptie van het management, obligatiehouders door het risicogedrag van de leiding en werknemers door onzekerheid in de loonruimte als gevolg van een verdoezeld bedrijfsresultaat.
De externe participanten (principalen) zullen zich deze gevaren terdege realiseren. Zij zullen hun agent (ondernemingsleiding) de verplichting opleggen verantwoording af te leggen over het gevoerde beleid, althans voor zover het hun belangen raakt. Hierdoor ontstaat de behoefte aan een specifiek oordeel omtrent de bruikbaarheid van de verantwoording. Dit oordeel kan het beste worden geveld door een deskundige, omdat het voor een principaal te duur zou zijn dit zelf te doen. De principaal huurt als deskundige de accountant in en verlaagt hierdoor zijn monitoring-kosten. Ergo, *de inzet van de accountant verlaagt hier de monitoring-kosten.*

Tegelijkertijd verkeren de externe participanten in een situatie die gekenmerkt wordt door een informatie-achterstand ten opzichte van de ondernemingsleiding. Gezien de economische rationaliteit zullen de externe participanten ervan uitgaan dat de ondernemingsleiding deze achterstand in haar voordeel zal gebruiken, ter realisering van haar eigen doeleinden, die kunnen afwijken van de doeleinden van de externe participanten. De externe participanten zullen, afhankelijk van de mate waarin zij denken te (kunnen) worden benadeeld, een hogere vergoeding vragen voor hun bijdrage in de onderneming. Het management zal daardoor de behoefte voelen de informatie-achterstand te verkleinen, als de kosten daarvoor tenminste lager zijn dan de te betalen hogere bijdrage voor de externe participanten. Indien dat het geval is *doet de accountant hier zijn intree als verlager van de bonding-kosten.*

De toegevoegde waarde van de accountant is aldus op een vrij eenvoudige manier te verklaren: doordat het werk en het produkt van de accountant de monitoring- en bonding-kosten verlagen, gaan de agency-kosten als geheel omlaag en blijft bij zowel de principalen als de agenten meer besteedbaar inkomen over. De Agency-theorie verklaart de accountantsfunctie dus uit een koele kosten/baten-analyse en niet zoals Limperg vanuit een maatschappelijk mandaat.

Op grond van het bovenstaande kan worden vastgesteld dat de Agency-theorie *een* fundament vormt van het beroep van accountant. Of deze theorie *het* fundament vormt kan slechts worden beantwoord als alle alternatieven worden bekeken. Dit valt buiten de scope van dit artikel.

De Agency-theorie als fundament voor het beroep van EDP-auditor

In de paragraaf over het ontstaan van de beroepen van accountant en EDP-auditor is aangegeven dat de inzet van computers vanaf de jaren zestig heeft geleid tot een grote afhankelijkheid van de automatisering en dat aldus de kwaliteit van de informatievoorziening veelal bepalend is voor een succesvol functioneren van organisaties. Aangegeven is dat organisaties zich steeds meer bewust zijn geworden en worden van de noodzaak van het adequaat beheersen van de automatisering, beter gezegd van de informatievoorziening. Naar voren is gekomen dat degenen die verantwoordelijk zijn voor het nemen van de automatiseringsbeslissingen en andere belanghebbenden moeite hebben met het beoordelen van de automatisering. Voor het vormen van een oordeel over de kwaliteit van de automatisering wordt vaak als deskundige de EDP-auditor ingeschakeld.

De EDP-auditor verlaagt in de Agency-theorie de monitoring-kosten van de principaal en bondingkosten van de agent. In tabel 1 zijn ter verduidelijking enkele voorbeelden gegeven van de beroepen die op de EDP-auditor worden gedaan in de terminologie van de Agency-theorie.
Elk contract beschrijft de verplichtingen waaraan beide partijen moeten voldoen en de sancties waaraan elke partij is onderworpen indien hij niet voldoet aan zijn contractuele verplichtingen.

Het in de vorige subparagraaf ten aanzien van de accountant gestelde geldt ook voor de EDP-auditor. Ook hij verlaagt de agency-kosten. Ter verduidelijking zal hier één van de in tabel 1 genoemde relaties worden beschreven.

Een onderneming gaat op een zeker moment over tot de aanschaf van een nieuw softwarepakket. Om te kunnen komen tot een definitieve keuze van een pakket start de onderneming een selectietraject. In dit selectietraject steunt de onderneming grotendeels op informatie die wordt verstrekt door de leveranciers van de softwarepakketten. Hierdoor ontstaat de behoefte aan een oordeel omtrent de bruikbaarheid van de door de leveranciers verstrekte informatie. Dit oordeel kan in sommige gevallen het beste worden geveld door een deskundige, omdat het voor een onderneming te duur zou zijn dit zelf te doen. De onderneming treedt dus op als principaal en de leverancier als agent. De principaal huurt als deskundige de EDP-auditor in en verlaagt hierdoor zijn monitoring-kosten. *De inzet van de EDP-auditor verlaagt hier de monitoring-kosten van de onderneming.*

Tegelijkertijd verkeert de onderneming in een situatie die gekenmerkt wordt door een informatie-achterstand ten opzichte van de leverancier inzake

Principaal	*Agent*	*Contract tussen principaal en agent*	*Opdracht aan EDP-auditor*
Gebruikers-organisatie	Interne automatiserings-afdeling (systeemontwik-keling en/of produktie)	Het leveren van de intern ontwikkelde software of de intern geleverde automatise-ringsdiensten	Geef een oordeel over de kwaliteit van de intern ontwik-kelde software of de intern geleverde automatiserings-diensten
Onderneming	Softwarehuizen	Het leveren van software	Geef een oordeel over de kwaliteit van de aangekochte software
De Neder-landsche Bank	Bankinstelling	Het verlenen van een vergunning voor het vestigen van een bank	Geef een oordeel over de betrouwbaarheid en de continuïteit van de geauto-matiseerde gegevens-verwerking

Tabel 1. Voorbeelden EDP-auditor in Agency-relaties.

de kwaliteit van software. De onderneming realiseert zich dat de leverancier deze achterstand in zijn eigen voordeel zal gebruiken, ter realisering van zijn eigen doeleinden, die kunnen afwijken van de doeleinden van de onderneming. De onderneming zal, afhankelijk van de mate waarin zij denkt hierdoor te (kunnen) worden benadeeld, een lagere vergoeding willen betalen aan de leverancier, bijvoorbeeld in de vorm van een lagere aankoopprijs, een hogere schadeloosstelling bij het niet nakomen van het contract door de leverancier of gratis correctief onderhoud. De leverancier zal daardoor de behoefte voelen de informatie-achterstand te verkleinen, als de kosten daarvoor tenminste lager zijn dan de lagere vergoeding die de onderneming wil betalen voor te leveren software. Hij geeft een EDP-auditor opdracht om een oordeel te geven over de kwaliteit van zijn software. *De EDP-auditor verlaagt de bonding-kosten van de leverancier.*

De EDP-auditor heeft dezelfde soort toegevoegde waarde als de accountant: het werk en het produkt van de EDP-auditor verlagen de monitoring- en bonding-kosten; de agency-kosten als geheel gaan omlaag en er blijft bij zowel de principalen als de agenten meer besteedbaar inkomen over. Op grond van het bovenstaande kan worden geconcludeerd dat de Agency-theorie *een* fundament vormt van het beroep van EDP-auditor.

'MANAGEMENT CONTROL'-BENADERING

De 'Management Control'-benadering staat centraal in de post-doctorale opleiding tot Register EDP-auditor aan de EUR. Hieronder volgt eerst een korte uiteenzetting van hetgeen op de EUR wordt verstaan onder de 'Management Control'-benadering. In de laatste subparagraaf zal ik nagaan of de 'Management Control'-benadering nieuwe elementen toevoegt aan de grondslagen van het beroep van EDP-auditor.

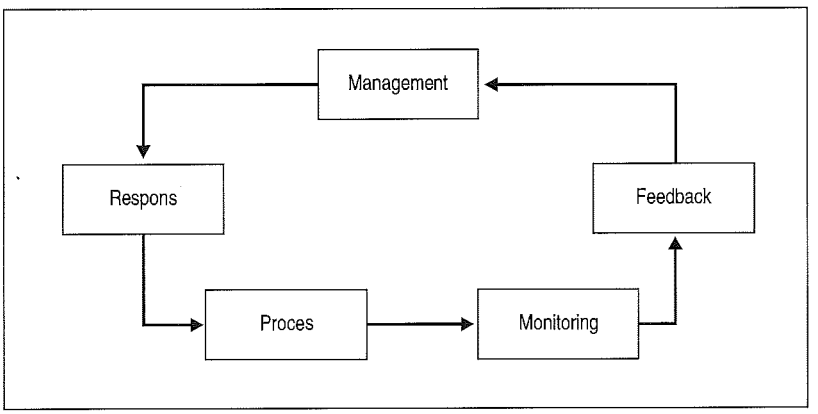
Uitleg 'Management Control'-benadering

Volgens Kocks ([Kock93]) bestaat een control-systeem uit drie delen:
- het monitoring-systeem;
- het feedback-systeem;
- het response-systeem.

Het monitoring-systeem omvat een stelsel van maatregelen om op grond van specifieke (controle)informatie vast te stellen dat processen, informatie en maatregelen voldoen aan door het management gestelde eisen. Het feedback-systeem omvat het volgens vaste regels informeren van het hogere echelon over de resultaten van de monitoring. Het response-systeem omvat de wijze waarop en de mate waarin het management op grond van feedback-informatie al dan niet overgaat tot bijsturing (input voor het engineering-proces).

In figuur 1 is een control-systeem weergegeven. Door in het schema van figuur 1 verschillende processen in te vullen wordt duidelijk dat control-systemen op verschillende niveaus binnen de organisatie voorkomen. Vaak maakt het control-systeem van een lager niveau deel uit van een te monitoren proces van een hoger niveau.

Het control-systeem waarmee het topmanagement van een onderneming wordt geïnformeerd over de



Figuur 1. Control-systeem.

wijze waarop de totale organisatie functioneert wordt het management control-systeem genoemd.

Accountant en management control

Nog steeds bestaat het grote deel van de werkzaamheden van de accountant uit het controleren van de betrouwbaarheid van de financiële verslaglegging. Binnen de accountancy is de laatste jaren de ontwikkeling ontstaan dat de accountant hierbij meer en meer aansluit op de beheersingswijze van de bedrijfsleiding van de risico's die de onderneming bedreigen. Deze ontwikkeling, zoals terug te vinden is in de controle-aanpak van eén groot aantal accountantskantoren, stelt de vraag centraal: 'Welke maatregelen heeft de bedrijfsleiding (management) getroffen om de bedrijfsprocessen te beheersen en de door haar gekozen doelstellingen te realiseren?'

Deze ontwikkeling is vooral ingegeven door economische motieven. De accountant is namelijk inmiddels van zijn voetstuk gehaald. Als gevolg van de toename van de mondigheid, een hoger opleidingsniveau, een groter aantal mensen dat deelneemt aan de informatieverstrekking en het feit dat vroeger onopgemerkte schandalen nu in de openbaarheid komen, kalft het van oudsher als vanzelfsprekend aangenomen gezag van de accountant langzaam af. Er is geen plaats meer voor blind vertrouwen in een beroepsgroep die een produkt aflevert dat maar heel moeilijk op toegevoegde waarde getoetst kan worden. Dit proces overkomt alle beoefenaren van vrije beroepen. Door de neerwaartse druk op de tarieven die de accountants bij zijn klant in rekening kan brengen, is de accountant op zoek gegaan naar mogelijkheden om zijn controle efficiënter te kunnen uitvoeren. Door de bovengenoemde vraag als uitgangspunt te nemen kan de accountant voldoende zicht krijgen op wat zich in de organisatie van zijn klant afspeelt.
Hierdoor laat de accountant aan zijn klant zien dat hij weet met welke vraagstukken het management zich bezighoudt. De accountant beperkt c.q. voorkomt hierdoor het risico van het ontstaan van een kloof tussen de toegevoegde waarde die klanten van hem/haar verwachten en de toegevoegde waarde die door hem/haar wordt geleverd c.q. kan worden geleverd.
Tevens vormt de wijze waarop het management zijn bedrijfsprocessen beheerst een aanknopingspunt voor de planning en de keuze van de controlemaatregelen gericht op het vellen van een oordeel over de getrouwheid van de jaarrekening.

De 'Management Control'-benadering biedt naast de Agency-theorie een mogelijkheid om het ontstaan van een kloof tussen datgene wat de samenleving verwacht van de accountant, en datgene wat de accountant de samenleving in feite biedt te verklaren. Op grond van het bovenstaande wordt geconcludeerd dat de 'Management Control'-benadering een steeds belangrijker grondslag vormt voor het accountantsberoep.

EDP-auditor en management control

In de paragraaf handelend over het ontstaan van de beroepen van accountant en EDP-auditor is gesteld dat de kwaliteit van de informatievoorziening veelal bepalend is voor een succesvol functioneren van organisaties. Daarnaast werd opgemerkt dat organisaties zich steeds meer bewust worden van de noodzaak van het in voldoende mate beheersen van de automatisering, beter gezegd van de geautomatiseerde informatievoorziening. Het management zal een stelsel van beheersmaatregelen moeten treffen c.q. via delegatie laten treffen om de kwaliteit van de geautomatiseerde informatievoorziening te kunnen waarborgen. Tevens zal het management een monitoring-systeem opzetten om vast te kunnen stellen dat de getroffen beheersingsmaatregelen qua opzet, bestaan en werking voldoende waarborgen bieden om de kwaliteit van de geautomatiseerde informatievoorziening te laten voldoen aan de door het management gestelde eisen. In toenemende mate geeft het management een EDP-auditor de opdracht om de opzet/het bestaan/de werking van de door het management getroffen beheersingsmaatregelen te beoordelen. Als reden waarom deze opdracht aan een EDP-auditor wordt verleend, kan worden genoemd de vereiste beschikking over specialistische kennis en ervaring, nodig voor een succesvolle uitvoering van deze opdrachten.

De EDP-auditor dient te voorkomen dat zijn beroepsgroep zich op hetzelfde voetstuk plaatst als de accountant. Als dit al wel heeft plaatsgevonden, dient de EDP-auditor zo snel mogelijk hiervan af te stappen om het ontstaan van een kloof tussen datgene wat de samenleving verwacht van de EDP-auditor, en datgene wat de EDP-auditor de samenleving in feite biedt, te voorkomen.

Door bij elke opdracht in eerste instantie zoveel mogelijk uit te gaan van de wijze waarop het management de risico's die de onderneming bedreigen tracht te beheersen, kan het risico worden beperkt dat de EDP-auditor te maken krijgt of reeds heeft met dezelfde verwachtingskloof als de accountant. Geconcludeerd wordt nu dat de 'Management Control'-benadering een belangrijke grondslag vormt voor het beroep van EDP-auditor.

DE RELATIE TUSSEN DE DRIE GRONDSLAGEN VAN HET BEROEP VAN EDP-AUDITOR

Ten slotte zal in deze paragraaf worden nagegaan of er een relatie is tussen de verschillende hiervoor genoemde grondslagen van het EDP-auditorsberoep, en zo ja, wat deze relatie inhoudt. Hiervoor zal een vergelijking worden gemaakt tussen enerzijds de 'Management Control'-benadering en anderzijds de Agency- en de Vertrouwenstheorie.

De Agency- en de Vertrouwenstheorie richten zich op een deel van het control-systeem: op het monitoring-systeem. Ook vormen beide theorieën slechts één van de mogelijke verschijningsvormen van het monitoring-systeem. In termen van de Agency-theorie kan het management gezien worden als de principaal die de EDP-auditor de opdracht verstrekt om het proces, dat wordt uitgevoerd door de agent, te monitoren en de resultaten in een bepaalde vorm naar het management terug te koppelen. Op de wijze waarop en de frequentie waarmee de terugkoppeling naar de principaal (het management) plaatsvindt wordt in de Agency-theorie niet ingegaan. Tevens wordt niets gezegd over de wijze waarop respons door het management zal plaatsvinden. In de Vertrouwenstheorie geven de externe participanten de accountant opdracht om de verantwoording van de ondernemingsleiding te monitoren. Overeenkomstig de Agency-theorie wordt bij de Vertrouwenstheorie geen invulling gegeven aan het feedback- en het response-systeem.

Op grond van het bovenstaande kom ik tot de conclusie dat de 'Management Control'-benadering met de introductie van het control-systeem nieuwe elementen toevoegt aan de grondslagen van het beroep van EDP-auditor. Beter gezegd, de 'Management Control'-benadering dient te worden gezien als een theorie van een hogere orde dan de Vertrouwens- en de Agency-theorie. De Vertrouwens- en de Agency-theorie geven een bepaalde inhoud aan een deel van de 'Management Control'-benadering.

Als slot kan samenvattend worden gesteld dat de 'Management Control'-benadering *het fundament* vormt van het beroep van EDP-auditor en dat de Vertrouwenstheorie van Limperg en de Agency-theorie *twee pijlers* van dit fundament vormen. De 'Management Control'-benadering geeft een adequaat raamwerk voor het identificeren van de verschillende soorten pijlers waarop het bestaansrecht van het beroep van EDP-auditor is gebouwd. Het identificeren van andere pijlers valt buiten de scope van dit artikel.

SAMENVATTING

In dit artikel is onderzocht of op het beroep van EDP-auditor dezelfde grondslagen van toepassing zijn als op het beroep van accountant en in hoeverre de 'Management Control'-benadering nieuwe elementen toevoegt aan de grondslagen van het beroep van EDP-auditor.

Eerst zijn de beide grondslagen van de accountantsfunctie beschreven: de Vertrouwenstheorie van Limperg en de Agency-theorie. Vervolgens is nagegaan in hoeverre de functie van EDP-auditor te herleiden is op deze grondslagen. Ten slotte wordt de relatie met de 'Management Control'-benadering besproken.

Volgens de *Vertrouwenstheorie van Limperg* is het optreden als vertrouwensman van het maatschappelijk verkeer de hoofdfunctie van de accountant. Limperg ziet de afnemer van het accountantsprodukt, de verstandige leek, in slechts één bepaalde hoedanigheid. Onder invloed van de economische, sociale en technologische ontwikkelingen heeft de verstandige leek in de loop der tijd vele hoedanigheden gekregen. Geconcludeerd is dat voor het overbruggen van de verwachtingskloof tussen accountants aan de ene kant en de samenleving aan de andere kant, afgestapt dient te worden van de termen 'verstandige leek' en 'maatschappelijk verkeer' zoals gedefinieerd door Limperg. De Vertrouwenstheorie kan dan ook nog steeds een fundament vormen voor het beroep van accountants indien de accountant zichzelf beschouwt als de vertrouwensman van *een deel van* het maatschappelijk verkeer. Het begrip 'verstandige leek' dient overboord te worden gezet. Het begrip 'maatschappelijk verkeer' kan wel worden gebruikt mits de volgende definitie wordt gehanteerd: 'het heterogene samenstel van individuen en organisaties dat invloed uitoefent op en/of gebruik maakt van de diensten van de accountant'.
De Vertrouwenstheorie van Limperg kan een fundament vormen voor het beroep van EDP-auditor mits de EDP-auditor het maatschappelijk verkeer ziet als een heterogeen samenstel van individuen en organisaties met elk hun eigen opvattingen en verwachtingen over de functie van de EDP-auditor. Indien de EDP-auditor dit niet doet, ontstaat een aanzienlijk risico dat hij te maken krijgt met dezelfde verwachtingskloof als de accountant.

De EDP-auditor dient te voorkomen dat zijn beroepsgroep zich op hetzelfde voetstuk plaatst als de accountant.

De tweede behandelde theorie tracht het bestaansrecht van het beroep van EDP-auditor te verklaren uit een bedrijfseconomische invalshoek: de *Agency-theorie.*
De EDP-auditor heeft volgens deze theorie dezelfde soort toegevoegde waarde als de accountant: het werk en het produkt van de EDP-auditor verlagen de monitoring- en bonding-kosten; de agency-kosten als geheel gaan omlaag en zo blijft voor zowel de principalen als de agenten meer besteedbaar inkomen over. Op grond van het bovenstaande is geconcludeerd dat de Agency-theorie een fundament vormt van het beroep van EDP-auditor.

Ten slotte is een derde theorie besproken, namelijk die welke centraal staat in de post-doctorale opleiding tot Register EDP-auditor aan de EUR, de *'Management Control'-benadering.* Door bij elke opdracht in eerste instantie zoveel mogelijk uit te gaan van de wijze waarop het management de risico's die de onderneming bedreigen tracht te beheersen, kan het risico worden beperkt dat de EDP-auditor te maken krijgt of reeds heeft met dezelfde verwachtingskloof als de accountant.

Geconcludeerd is dat de 'Management Control'-benadering een belangrijke grondslag vormt voor het beroep van EDP-auditor.
De 'Management Control'-benadering vormt een adequaat raamwerk voor het identificeren van de verschillende soorten pijlers waarop het bestaansrecht van het beroep van EDP-auditor is gebouwd.

Samenvattend is geconcludeerd dat de 'Management Control'-benadering *het* fundament vormt van het beroep van EDP-auditor en dat de Vertrouwenstheorie van Limperg en de Agency-theorie twee pijlers van dit fundament vormen.

LITERATUUR

[Blok91b] Blokdijk, H., *De verwachtingskloof: dempen of overbruggen?*, Maandblad voor Accountancy en Bedrijfshuishoudkunde, april 1991.

[Blok91b] Blokdijk, J.H., *Strategieën bij de verwachtingskloof*, Maandblad voor Accountancy en Bedrijfshuishoudkunde, december 1991.

[Bruij93] Bruijn, A. de, *EDP-auditing, wat is het?*, de EDP-Auditor, 2e jaargang nr. 2, april 1993.

[Dass89] Dassen, R.J.M., *De leer van het Gewekte Vertrouwen: Agency avant la lettre?*, Maandblad voor Accountancy en Bedrijfshuishoudkunde, september 1989.

[Frie93] Frielink, A.B., *EDP-auditing, welke inhoud geven we daaraan?*, de EDP-auditor, 2e jaargang nr. 3, juli 1993.

[Heijd94] Heijden, H. van der, *Toepassingen van de agency-theorie in de bestuurlijke informatiekunde*, Informatie, jaargang 36 nr. 2.

[Kock93] Kocks, H.C., *Inzicht en samenhang*, Rotterdam, Erasmus Universiteit Rotterdam, 1993.

[Moer92a] Moerland, P.W., *Economische theorievorming omtrent de onderneming (deel 1)*, Maandblad voor Accountancy en Bedrijfshuishoudkunde, januari/februari 1992.

[Moer92b] Moerland, P.W., *Economische theorievorming omtrent de onderneming (deel 2)*, Maandblad voor Accountancy en Bedrijfshuishoudkunde, maart 1992.

[NIVR89] Automatisering en controle: Deel VII. *Kwaliteitsoordelen over de informatievoorziening*, NIVRA-geschrift nummer 53, november 1989.

[NIVR91] NIVRA, *De accountantsverklaring; tekst en uitleg*, brochure, 1991.

[NIVR94] NIVRA, *Verordening Gedrags- en Beroepsregels Registeraccountants*, NIVRA 1994, artikel 11-17.

[NIVR1] NIVRA, *1.01 Algemeen kader met betrekking tot controle en daaraan verwante opdrachten*, RADAR Richtlijnen Controle, RC 0.01-1.

[NIVR3] NIVRA, *5.03 De accountantsverklaring*, RADAR Richtlijnen Controle, RC 5.03-1-19.

[NIVR4] NIVRA, *5.04 Onzekerheden en bedenkingen*, RADAR Richtlijnen Controle, RC 5.04-1-13.

[Opho90] Ophof, *De accountant: agent of vertrouwensman?*, Maandblad voor Accountancy en Bedrijfshuis-houdkunde, september 1990.

[Sijbr96] Sijbring, H.E., *De EDP-auditor: vertrouwensman, agent of .....?*, Afstudeerreferaat voor de post-doctorale opleiding tot Register EDP-auditor aan de Erasmus Universiteit Rotterdam (EUR), 2 februari 1996.

[Limp32,33] Limperg jr., Th., *De functie van den accountant en de leer van het gewekte vertrouwen*, artikelreeks in Maandblad voor Accountancy en Bedrijfshuishoudkunde, februari 1932, oktober 1932, oktober 1933 en november 1933.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder ISBN 90 14 04634 0.

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
Drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeemontwikkeling
Drs. J.J. van Beek RE RA

Audit automation
Drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
Mw.mr.drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
Drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
Drs. R. Oudega en drs. P. Veltman RE RA

1 21e jaargang 94/1 lente 1994

De invloed van informatietechnologie op de beheersing van organisaties
Prof. A.W. Neisingh RE RA

Rekencentra: normen voor menskracht
Prof.dr.ir. R. Paans RE

Accountant en de kosten- en batenbeheersing van informatietechnologie
Prof. H.B. Moonen RE RA

Informatiebeveiliging: de tijd is rijp
Drs. H.G.Th. van Gils RE RA

Het beoordelen van het testen van systemen
P. van Berge

2 21e jaargang 94/2 zomer 1994

Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI

Beveiliging van analoge kieslijnen
Drs.ing. D. Brouwer RE

Beveiliging van UNIX
Mw.drs. M.C. van Lith RE

Typologie van workflow-managementsystemen
Drs. D.J.P. Witte

3 21e jaargang 94/3 herfst 1994

Inleiding tot op TCP/IP gebaseerde netwerken
Ir. P. Kornelisse

Internet? Maar dan wel met een firewall!
H. van Hulst

Netwerkverbindingen in een OpenVMS-omgeving
Ir. J.H. Lie-Tjauw

Enige juridische wegwijzers voor de elektronische snelweg
Mw.mr. G.P. van Duijvenvoorde

Betrouwbaarheid en beveiliging van een CICS-omgeving
Ing. G.H.M. Meijer RE en mw. J.A.M. Holla

4 21e jaargang 94/4 winter 1994

Geautomatiseerde gegevensbewerking en jaarrekeningcontrole
R.A. Jonker RA

De invloed van informatietechnologie op de interne-controleprincipes
J.C. Boer RE RA

Audit van een logistiek systeem
Drs. J.A.C. van Geel, ing. A.P.J. Mouwen en drs. E.P.R. van Vroenhoven RE RA

Informatiebeveiliging van theorie naar praktijk
Drs. P. Veltman RE RA

Informatie(beveiligings)beleid in concernverband
Prof. A.W. Neisingh RE RA

1 22e jaargang 95/1 lente 1995

Internetworking; beheerproblematiek en security-risico's
H. Roos RA en ir. M.T.H. Heesbeen

Geïntegreerd netwerkbeheer
Ing. W.A.A. Zoon

Client/server geconcretiseerd
J.C. van Praat RE RA

Radio-LAN's in de praktijk
Ir. B.J. Busropan, ir. G.J. de Groot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor

3DAS-kenmerk, een uniek middel voor identificatie en authenticatie
Ir. W.H.M. Sipman RI

2 22e jaargang 95/2 zomer 1995

Het beheer van PC-netwerken
Drs.ing. R.F. Koorn CISA

Multimedia nader bekeken
Drs. A.M. Buren

Introductie van een bancair systeem in een wide area netwerkomgeving
W.N.P. Zethof RE RA

GEBIT. Gestructureerd Evalueren van de Baten van IT-investeringen
Mw. M.S. Hablous

3 22e jaargang 95/3 herfst 1995

Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering
Mw. W.A. de Munck RA

Plaats en taken van de EDP-auditfunctie bij de KLM
J.G. de Vries RE RA

Wet op het consumentenkrediet: systeemgericht onderzoek vereist
R. van den Hoorn RA

Third party review en -mededeling bij uitbesteding van IT-services
Drs. P. Veltman RE RA

Maatwerk past informatiebeveiliging
Drs. E. Roos Lindgreen en mw.drs. C. Schönfeld RI

Stroomlijnen en herontwerpen in een onderhoudsbedrijf: gelijktijdig en/of volgtijdig?
Drs. O.C. van Leeuwen RA en drs. M.C. van Veen RC

Het ontwikkelen van methoden en technieken van EDP-auditing
Drs. R.G.A. Fijneman RE RA

4 22e jaargang 95/4 winter 1995

Informatieplanning en standaardpakketten
Drs. J. de Boer en ir. J.A.M. Donkers RE

Certificatie van een standaardpakket voor financiële administraties
Drs. H.G.Th. van Gils RE RA

AO en standaardpakketten: integratie verhoogt de kans op een succesvolle selectie en implementatie
Drs. J.J. van Beek RE RA, drs. W. Boogaard RA CPIM en drs. J.J.B. van den Oever

Waardebepaling van software
Ir. J.A.M. Donkers RE en drs. G.J.J. Timmer

Business Process Controlling
Drs. J.J. van Beek RE RA en W. Teeuwissen RA

1 23e jaargang 96/1

Normbesef
L. Annokkée RE en B. Sebregts RE

ISO 9000 en EDP-auditing
Mr. W.R. Nanninga RE en ltkol J.M.W. van de Garde RE

ITIL als inrichtings- en beoordelingsinstrument
Drs. F.J. Hut

De Code voor Informatiebeveiliging
Dr.ir. P.L. Overbeek

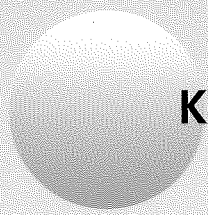
De Code voor Informatiebeveiliging als norm voor de EDP-auditor
W.S.C. Krol RE en drs. M.M. Smits

2 23 jaargang 96/2

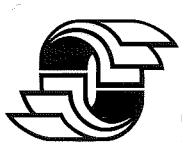
Besluitvorming over IT-investeringen: gebruik de juiste criteria
Ing. E.M.H. Coorens BE MBA, drs. P.J.C. van Bladel en dr. M. Boogaard

Benchmarking, een hulpmiddel voor de EDP-auditor?
Ir. J.A.M. Donkers RE en mw. ir. E.R. van Sommeren

AS/400-networking
Mw. drs. A.L. Hristova RE



KPMG EDP Auditors



Samsom BedrijfsInformatie