# COMPACT

TIJDSCHRIFT EDP-AUDITING

## ERP-PAKKETTEN EN DE TOEGEVOEGDE WAARDE VAN IT-TRENDS

1997/3

**Compact ®**
*Jaargang 24, 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*
*Mr. P. van Dijken*
*G. van Essen RA*
*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**
*Dr. J.H. Elich*

*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.*

*Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom Bedrijfsinformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.*

*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.*

## REDACTIONEEL

De vorige Compact (1997/2) stond al volledig in het teken van het onderwerp standaardpakketten. Daarbij is onder andere ingegaan op de te volgen aanpakken bij het selecteren en implementeren van dergelijke pakketten.
Het blijkt dat pakketten verschillend zijn gestructureerd. Niet alleen qua functionaliteit maar ook qua technologie. Hierdoor is het selectie- en implementatieproces vaak lastig uitvoerbaar. De eindgebruiker wordt met vele veranderingen geconfronteerd en ook met voor hem of haar onbekende technologische begrippen. Het in goede samenhang met elkaar vergelijken van de verschillende oplossingsmogelijkheden wordt daardoor complex. Het effect kan zijn dat onduidelijke besluitvormingsvoorstellen worden voorgelegd aan het management of – nog erger – dat zelfs een geheel verkeerde oplossing wordt gekozen.

Twee artikelen in deze Compact proberen voor eindgebruikers c.q. managers de inzichtelijkheid in het complexe selectie- en implementatieproces te vergroten. Gepleit wordt voor een tweedeling in de implementatie, zodat populair gezegd niet alles in één keer op zijn kop gaat. Na een basisimplementatie kan verder worden verfijnd. Om grip te krijgen op allerlei moderne automatiseringsbegrippen (IT-trends) wordt de toegevoegde waarde van deze trends voor het functioneren van een standaardpakket toegelicht. Daarbij wordt de invalshoek gekozen van wat de eindgebruiker op zijn of haar werkplek merkt van de nieuwe technologie.

De vele oriëntaties op en implementaties van standaardpakketoplossingen zijn in het vorige Redactioneel in het licht van het gezonde economische klimaat geplaatst. Andere motieven zijn echter ook aanwezig. Een belangrijk motief momenteel is het naderende Jaar 2000-probleem. Huidige applicaties blijken regelmatig niet te voorzien in een oplossing voor de millenniumovergang. De investeringen benodigd voor het aanpassen van de software kunnen aanzienlijk zijn. Managers proberen momenteel twee slagen in één te slaan. De keuze voor een standaardpakket kan de organisatie functioneel en beheertechnisch vooruithelpen en tevens kan het Jaar 2000-probleem, mits het pakket tijdig wordt geïmplementeerd, worden opgelost. Voor organisaties die dit pad niet kunnen bewandelen, wordt het beheer van Jaar 2000-projecten nader belicht.

Bij de inrichting van een standaardpakket spelen beheervraagstukken een belangrijke rol. De wijze waarop de administratieve organisatie en interne controle kunnen worden ingericht, is afhankelijk van de faciliteiten die het pakket daarvoor biedt. Een pakketmededeling over de kwaliteit van de software kan daarbij behulpzaam zijn. Uitgebreid wordt in het artikel over pakketmededelingen beschreven hoe dergelijke audits dienen te worden uitgevoerd en op welke wijze de rapportage hieromtrent dient plaats te vinden.
Een andere beheercomponent betreft de inrichting van de informatiebeveiliging. Indien toch als onderdeel van de pakketimplementatie de beheerstructuur opnieuw wordt geijkt en ingericht, is ook aandacht voor informatiebeveiliging aan de orde. Een systematische aanpak zoals beschreven in het Voorschrift Informatiebeveiliging Rijksdienst verdient dan de voorkeur.

Uit het bovenstaande blijkt dat pakketselecties en -implementaties diverse veranderingsvraagstukken oproepen. Niet alleen betreft dit functionele vragen, maar ook organisatorische, financiële en kwaliteitsvragen. Dit maakt het niet alleen voor de organisatie tot een uitdaging, maar ook voor de EDP-auditor die zich als IT-consultant kan en wil profileren.

Drs. R.G.A. Fijneman RE RA

# Maximaal rendement uit een geïntegreerd standaardpakket

Drs. M.A.A. Jongen,
R.L.M. Essers en
drs. E.P.R. van Vroenhoven RE RA

**De implementatie van een standaardpakket kan worden gesplitst in een basisimplementatie en een optimalisatiefase. Hierdoor is het mogelijk de risico's tijdens de uitvoering van het project te reduceren. Door de veelheid aan keuzen, de sterke integratie van de modules en de sterke relaties met de organisatievraagstukken blijkt namelijk dat implementatieprojecten complex kunnen zijn. Een 'vernieuwde' aanpak staat centraal in de behandeling.**

## INLEIDING

De laatste jaren start een toenemend aantal bedrijven een herautomatiseringstraject met behulp van standaardpakketten. Steeds vaker worden standaardpakketten toegepast als automatiseringsoplossing in plaats van, door zelfbouw, maatwerk te realiseren. Dit wordt onder andere ingegeven doordat de technologische ontwikkelingen steeds sneller op elkaar volgen. Deze ontwikkelingen kunnen alleen door middel van standaardpakketten worden bijgehouden. Ook speelt het geïntegreerde aspect van veel pakketten een rol bij de keuze tussen maatwerk en standaardpakketten; geïntegreerde pakketten stellen organisaties immers in staat overbodige processtappen te elimineren en verantwoordelijkheden op de juiste plaats toe te kennen. De gevraagde functionele complexiteit kan niet worden gerealiseerd zonder specialistische kennis. Het is moeilijk en meestal niet rendabel om deze kennis binnen een bedrijf op te bouwen en vast te houden. De softwarehuizen beschikken in ieder geval wel over deze specialistische kennis.

De aanschaf en implementatie van een standaardpakket vergt een hoge investering. Vanzelfsprekend wenst het management zekerheid dat het pakket bijdraagt tot een betrouwbare en effectieve bedrijfsvoering. Projecten gericht op implementatie van standaardpakketten zijn in de praktijk gezien hun aard vaak risicovolle projecten. Pakketten introduceren vaak nieuwe werkwijzen en daarmee organisatieveranderingen. Geïntegreerde pakketten raken vele afdelingen en medewerkers, en standaardpakketten zijn door parameterinstellingen, schermaanpassingen, interfaces en dergelijke vaak niet zo standaard als de term zou doen vermoeden.

Een optimaal uitgevoerd implementatieproject is een belangrijke randvoorwaarde voor het behalen van maximaal rendement uit een investering in een geïntegreerd standaardpakket. Een optimale inrichting vormt de basis voor een optimale uitvoering van het implementatieproject.
In dit artikel zal een nieuwe aanpak van implementatie worden gepresenteerd.

## GEEN OPTIMALE IMPLEMENTATIE: GEEN MAXIMAAL RENDEMENT

Een nieuw geïntegreerd standaardpakket selecteren en dit vervolgens 'even' implementeren lijkt eenvoudig, maar de praktijk wijst uit dat weinig bedrijven kunnen verhalen over een soepel verlopen implementatieproject. Ook al wordt een implementatieproject als geslaagd betiteld, achteraf blijkt vaak dat het nieuwe systeem slechts een *imitatie is van het 'oude' systeem.* Alleen het onderhoud is buiten de deur gebracht (bij de softwareleverancier) en een grafische user interface en nieuw technisch platform zijn gerealiseerd.

*Voorbeeld 1. Geen optimale pakketimplementatie.*

Eén van de redenen waarom bedrijven overgaan tot het implementeren van een nieuw logistiek standaardpakket is dat met het huidige systeem de benodigde stuurinformatie (onder andere managementinformatie) niet of niet snel genoeg kan worden geproduceerd.
In de *oude situatie* is vaak sprake van eilandautomatisering wat inhoudt dat de systeembeheerder gegevens uit deelsystemen verzamelt met behulp van speciale zoek- en sorteerprogramma's. Hierdoor ontstaan relatief lange doorlooptijden om te kunnen reageren op ad-hocvragen vanuit de organisatie.
Pas *na* implementatie van een nieuw systeem blijkt dat de project- en werkgroepen geen tijd hebben gehad voor het definiëren van de juiste stuurinformatie; het definiëren van rapportages wordt doorgeschoven naar een volgende projectfase. Het gevolg hiervan is dat gebruikers zelf met nieuwe ter beschikking gestelde tools (report writers, query tools, etc.) ad-hocrapporten gaan aanmaken die vervolgens niet op elkaar aansluiten. Tevens blijkt niet te zijn nagedacht over de performancekwestie van het overdag rapporten genereren.

*Bij de selectie* van een nieuw standaardpakket heeft een bepaald bedrijf de aanwezigheid van een adequaat verkoopinformatiesysteem zwaar laten wegen.
*Na de implementatie* blijkt dat het systeem niet goed is ingericht en tevens is een aantal procedures niet opgesteld, waardoor onder andere de prospect- en de concurrentinformatie niet of onvoldoende worden bijgehouden; tevens worden de bezoekrapportages en actielijsten niet adequaat bijgehouden. Hierdoor biedt het nieuwe systeem weinig toegevoegde waarde.

*Voorbeeld 2. Geen optimale pakketimplementatie.*

Deze voorbeelden zijn voorbeelden waarbij het nieuw geïntegreerde standaardpakket de bedrijfsprocessen *niet optimaal* ondersteunt. Het nieuwe systeem wordt niet optimaal ingezet of ingericht. Echte procesverbetering, gerelateerd aan de mogelijkheden van het nieuw geïntegreerde standaardpakket, wordt onvoldoende gerealiseerd.

In toenemende mate worden door organisaties EDP-auditors ingeschakeld om na een implementatie een zogenaamde post implementation review uit te voeren. De aanleiding hiervoor is dat of de operationele procesgang is verstoord of de directie onvoldoende rendement waarneemt. De directie heeft sterke aanwijzingen dat dit wordt veroorzaakt door een niet-optimale pakketimplementatie. Op basis van de resultaten van de post implementation review worden additionele activiteiten uitgevoerd gericht op de verbetering van het systeem om alsnog het investeringsrendement uit het standaardpakket te verbeteren. De schade is echter reeds aangericht. Het totale project inclusief de verbeterperiode kent een langere doorlooptijd, waardoor de terugverdientijd van de investering langer wordt dan vooraf ingeschat. Bovendien kan bij de gebruikers een moeilijk omkeerbare aversie tegen het systeem ontstaan met daaruit volgende problemen voor het doorvoeren van de vereiste organisatorische veranderingen. Het is dus belangrijk te voorkomen dat een dergelijke situatie ontstaat.

Voordat dit artikel nader ingaat op de oorzaken van een niet-optimale pakketimplementatie is het noodzakelijk dat eerst wordt beschreven wanneer een pakketimplementatie dan wel als optimaal kan worden gekarakteriseerd.

De essentie van een optimale implementatie is een zo kort mogelijke terugverdientijd en realisering van maximale baten uit de investering in het standaardpakket.
Hiertoe dient te worden voldaan aan een aantal vereisten, te weten: een korte doorlooptijd en optimaal gebruik van de mogelijkheden en oplossing van de beperkingen van het systeem. Het optimaal gebruik van het systeem kan onder andere worden gerealiseerd door voldoende pakketkennis in de organisatie en een optimale stroomlijning van de organisatie gebaseerd op de door het nieuwe systeem geboden mogelijkheden. Het vaak voorkomende woord 'optimaal' kan worden geïnterpreteerd als juist gedoseerd en maximaal haalbaar gezien de (IT-)volwassenheid en -potentie van de organisatie.

## OORZAKEN VAN NIET-OPTIMALE PAKKETIMPLEMENTATIE

Om oplossingsrichtingen te zoeken voor niet-optimale pakketimplementaties is het belangrijk nog wat meer in detail op een aantal oorzaken in te gaan.

*Systeem onvoldoende afgestemd op organisatie*
Onvoldoende fine-tuning en focus op de specifieke organisatie leidt tot een verkeerde inrichting van het systeem. Vaak wordt dit geïnitieerd door onvoldoende 'echte' betrokkenheid van de organisatie bij het implementatietraject. Niet goed toepasbare functionele concepten worden geïmplementeerd. De specifieke kenmerken van de processen van de organisatie zijn onvoldoende terug te vinden. Het systeem is te 'standaard' ingericht.

*Te veel functionaliteiten*
Een ander veel voorkomend fenomeen is dat bedrijven direct te veel nieuwe functionaliteiten van het systeem willen gaan benutten. Bij aanvang van het project is vaak geen duidelijke afbakening van te implementeren functionaliteiten gemaakt. Het bedrijf raakt in de ban van de vele functionaliteiten die nieuwe pakketten bieden en de gestelde doelen worden uit het oog verloren: men gaat te ambitieus van start. Nieuwe functionele concepten worden ingevoerd hetgeen tot ingrijpende organisatorische veranderingen leidt waar de organisatie nog niet

aan toe is. De complexiteit van de implementatie wordt te groot waardoor doorlooptijden en budgetten onder druk komen te staan. Om vervolgens toch de implementatie binnen redelijke tijd af te ronden, worden projectdoelstellingen bijgesteld. Van een duidelijke prioriteitstelling inzake het nastreven van de doelstellingen is echter geen sprake meer. Door de doorlooptijd en complexiteit van het project is bovendien de energie voor latere invoering van extra functionaliteiten en verdere verbeteringen afgenomen. Er is sprake van 'goal reduction'.

*Onvoldoende aandacht voor verandering van de huidige werkwijze*
In dit geval wordt het pakket geïntroduceerd zonder in voldoende mate de huidige werkwijze aan de kaak te stellen. De veranderingen als gevolg van het systeem worden niet op doordachte wijze in een nieuwe werkwijze gegoten en uitgedragen. De voor maximaal rendement benodigde veranderingen van de huidige werkwijze worden vervolgens op de lange baan geschoven. De organisatie beklaagt zich vervolgens dat het systeem niet goed aansluit op de (bestaande) manier van werken. Het systeem biedt de mogelijkheden tot verandering met positieve baten. De organisatie heeft deze mogelijkheden echter niet aangegrepen, waardoor de investering nutteloos is geweest.

*Onvoldoende aandacht voor kennisopbouw*
Een andere belangrijke oorzaak voor het ontstaan van een niet-optimale pakketimplementatie is het onderschatten van de consequenties van de introductie van nieuwe functionaliteiten, werkwijze en schermen. De gebruikers kunnen nog enigszins wennen aan het nieuwe systeem (verandering automatisering), echter gecombineerd met een andere werkwijze en eventueel nieuwe functionele concepten kan het gebeuren dat er binnen korte tijd te veel kennis moet worden opgebouwd.

Bovenstaande oorzaken van een niet-optimale pakketimplementatie zijn in feite te herleiden tot onvoldoende afstemming tussen de organisatorische en systeemtechnische veranderingen. Beide dienen geïntegreerd in hetzelfde tempo te worden uitgevoerd om het resultaat na implementatie optimaal te laten zijn. Het realiseren van het beoogde effect van organisatorische en daarmee systeemtechnische veranderingen is afhankelijk van een goede begeleiding (veranderingsmanagement) en een gefaseerde uitvoering. De grootte van te nemen stappen is afhankelijk van de organisatie. Aspecten als automatiseringsgraad, veranderingspotentie, cultuur en gebruikersniveau spelen hierin een belangrijke rol.

Een vorm van een dergelijke stapsgewijze c.q. gefaseerde implementatie wordt in dit artikel beschreven. Hierbij wordt uitgegaan van een tweetal stappen c.q. fasen. In de eerste fase wordt *'basisfunctionaliteit'* in gebruik genomen die sterk aansluit bij de huidige werkwijze. Daarna volgt een optimalisatiefase waarin die functionaliteit verder wordt uitgebouwd en het gebruik van het systeem alsmede de inrichting van de organisatie begeleid wordt geoptimaliseerd.
Hierdoor worden de gebruikers in de gelegenheid gesteld om reeds in een vroeg stadium 'hands-on'-ervaring met het systeem op te doen. Dit bevordert de acceptatie en het veranderingsvermogen voor de optimalisatiefase. Tijdens de optimalisatiefase wordt het dan geldende maximale rendement uit het pakket gerealiseerd en dit alles binnen aanvaardbare doorlooptijd, onder andere vanwege het vooraf duidelijk plannen en het afbakenen van beide fasen.

*Voorbeeld 3. Onvoldoende afstemming tussen organisatie en systeem.*

Indien een volledig voorraadgestuurd bedrijf via de implementatie van een pakket een ordergestuurde eindassemblage wil introduceren, komen ter realisering van de verwachte baten diverse organisatorische veranderingen aan de orde. Naast het omgaan met een nieuw pakket met daarbij behorende functionaliteiten zoals Final Assembly Scheduling (FAS), Master Production Scheduling (MPS) en Available to Order (AtP) is een volledig andere werkwijze aan de orde.
Planning heeft in plaats van één, twee planningsniveaus (FAS en MPS); Engineering zal modulair moeten ontwerpen met meervoudig gebruik van dezelfde onderdelen in eindproducten, wil de invoering voorraadverlagende effecten hebben; de doorlooptijd bij eindassemblage dient adequaat te worden beheerst om aan de gewenste levertijden te kunnen voldoen, en dergelijke.
Wanneer vooraf onvoldoende aandacht wordt geschonken aan bovenvermelde aspecten, of indien de organisatie daar nog niet aan toe is, is invoering van het FAS-principe niet zinvol.

Succesvolle invoering van 'automatische factuurcontrole'-functionaliteit vereist nogal wat organisatorische randvoorwaarden. Zo moeten tijdige invoer van inkooporders met juiste prijzen en juiste toewijzing aan bijvoorbeeld kostenplaatsen worden gerealiseerd. Tevens moeten de goederenontvangsten tijdig worden ingevoerd. Indien onvoldoende aandacht wordt besteed aan de realisatie van deze organisatorische randvoorwaarden is invoering van het automatische factuurcontroleprincipe niet zinvol. Voorziene baten ter realisering van fte-capaciteit voor factuurcontrole worden niet gerealiseerd.

*Voorbeeld 4. Onvoldoende afstemming tussen organisatie en systeem.*

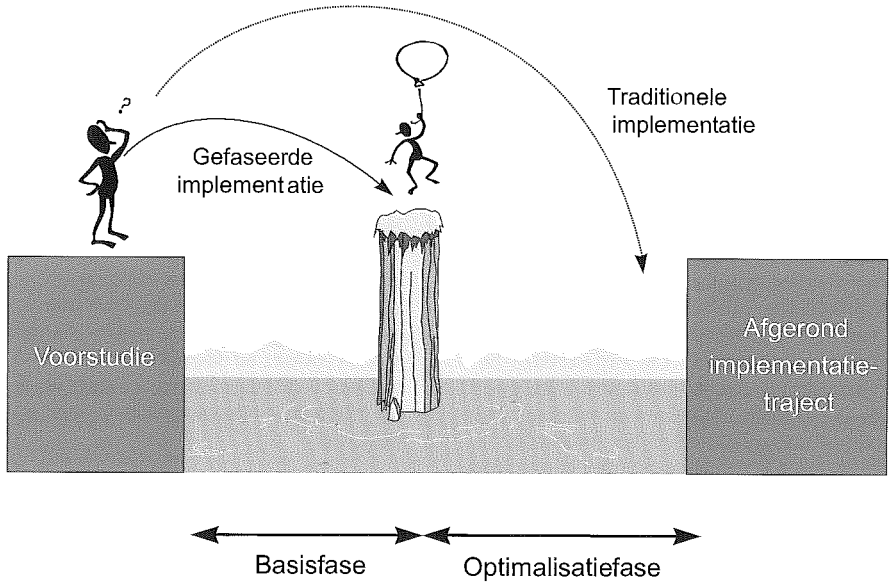
## DE GEFASEERDE IMPLEMENTATIE-AANPAK

De gefaseerde implementatieaanpak is, zoals zojuist beschreven, een aanpak om standaardpakketten te implementeren in twee deelfasen, de basisfase en de optimalisatiefase. Deze gefaseerde aanpak tracht de in de vorige paragraaf beschreven oorzaken van niet-optimale pakketimplementaties te voorkomen.

**Basisfase: enkele karakteristieken**

Kenmerkend voor de basisfase is dat in een relatief korte doorlooptijd een 'werkend systeem' wordt neergezet. Deze korte doorlooptijd wordt mogelijk gemaakt door het streven naar minimale complexiteit gedurende de basisfase. Enerzijds houdt dit in het beperken van organisatorische veranderingen. De organisatiefocus ligt op het leren bedienen van het nieuwe systeem. De introductie van nieuwe concepten en grote herstructureringen van de organisatie worden uitgesteld tot de optimalisatiefase. Anderzijds en natuurlijk aansluitend hierop wordt de inzet van functionaliteit beperkt tot met name op dit moment aanwezige basisfunctionaliteit. Onder basisfunctionaliteit wordt die functionaliteit

De overgang van de huidige situatie naar een situatie met een volledig geïmplementeerd standaardpakket kan worden gesymboliseerd als een sprong over een (brede) sloot waar de linkeroever de situatie vóór implementatie voorstelt en de rechteroever het einde van het project (een optimaal geïmplementeerd pakket). Doel van de implementatie is een sprong van rechter- naar linkeroever zonder hierbij een nat pak te halen. In de traditionele aanpak wordt geprobeerd in één keer over de sloot te springen (veelal met een nat pak als gevolg), terwijl de hier beschreven aanpak pleit voor een sprong met een tussenlanding op een eiland.



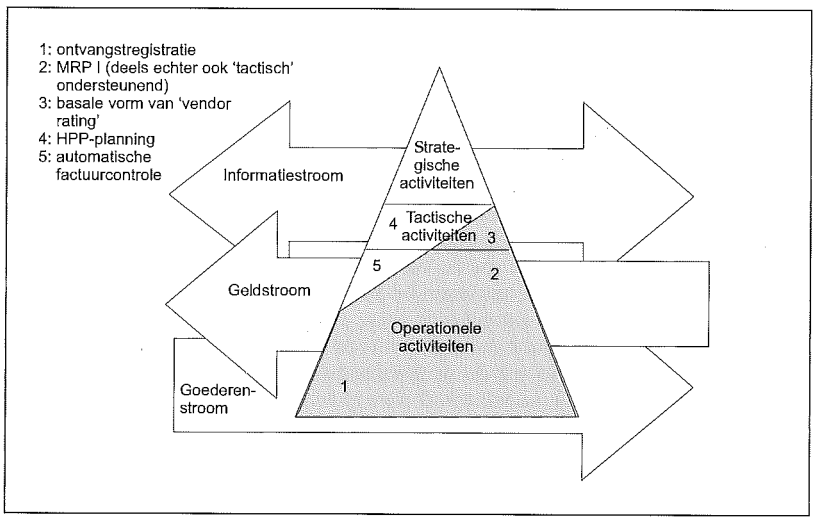

*De gefaseerde implementatieaanpak.*

verstaan die met name *de operationele activiteiten en daarmee de geld- en goederenstroom door de organisatie ondersteunt* (zie ook figuur 1).

In de volgende paragraaf wordt nader ingegaan op het vaststellen van de scheiding tussen basis- en optimalisatiefase.

Om een korte doorlooptijd te kunnen realiseren en bovendien uitgaande van het principe dat basisfunctionaliteit wordt geïmplementeerd, is de inzet van implementatietools in de basisfase essentieel. Zo hanteert bijvoorbeeld softwareleverancier Baan het tool 'Dynamic Enterprise Modeler'. Dit tool biedt een breed scala van voorgedefinieerde bedrijfsprocessen met daarbij te hanteren werkwijzen indien gebruik wordt gemaakt van de Baan-software. Ervan uitgaande dat basisprocessen en daarmee basisfunctionaliteiten in een bepaald bedrijfstype (bijvoorbeeld Assembly to Order) relatief standaard zijn, kan met behulp van dergelijke tools de basisfase worden verkort. Dergelijke tools kunnen bovendien worden gebruikt om het leerproces, één van de doelstellingen van de basisfase, te ondersteunen. Vanuit processchema's (flowcharts) kan door de gebruiker naar schermen in de software worden 'gesprongen'. Dit geschiedt door het activeren van een activiteit in het processchema (bijvoorbeeld de activiteit 'Invoeren verkooporder'), waarna het desbetreffende scherm (Verkooporders Invoerscherm) binnen de software wordt opgeroepen. De gebruiker verkrijgt op deze wijze een duidelijker beeld met welk proces en welke activiteiten daarbinnen hij bezig is.

*Figuur 1. Model ondersteuning van activiteiten.*




De implementatie van de basisfunctionaliteiten wordt sterk gedreven door pakketspecialisten. De bedrijfsprocessen worden in samenwerking met enkele eindgebruikers door het tool gemodelleerd, waarna de pakketspecialisten het pakket verder parametriseren en basisrapporten en documenten als facturen organisatiespecifiek opleveren. De organisatie wordt daarna intensief betrokken bij het testen van c.q. de opleiding in het pakket.

**De optimalisatiefase: enkele karakteristieken**

De optimalisatiefase beoogt het basissysteem uit te breiden en het gebruik te optimaliseren.
Een en ander vindt zijn neerslag in de specifieke projectstructuur voor deze fase. Gedurende de optimalisatiefase worden verschillende deelprojecten

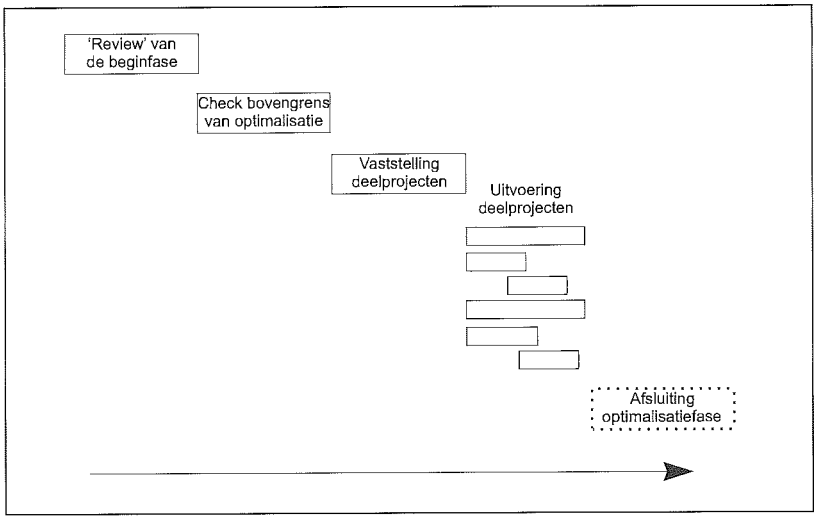
uitgevoerd, die parallel aan elkaar kunnen plaatsvinden.

Het aantal en het soort projecten die tijdens de optimalisatiefase worden uitgevoerd, is afhankelijk van de organisatie. Projecten zijn enerzijds gericht op optimalisatie van tijdens de basisfase geïmplementeerde functionaliteiten. Een voorbeeld is het verbeteren van de kwaliteit van MRP (Material Requirement Planning). Hiertoe worden bijvoorbeeld de basisgegevens voor MRP uitgebreid onder de loep genomen en verbeterd. Een ander voorbeeld is de verbetering van het goederenontvangstproces. Welke artikelen moeten voor inslag worden gekeurd, welke afkeurregistratie kan het beste worden gehanteerd en hoe kan in de organisatie en met het systeem optimaal met afkeur en daarmee retouren worden omgegaan.
Anderzijds bestaan projecten uit het implementeren van compleet nieuwe functionaliteiten of modules. Een voorbeeld van dit soort projecten is de invoering van FAS-functionaliteiten (Final Assembly Scheduling) en een productconfigurator. Deze worden door een bedrijf geïmplementeerd bij overgang van een voorraadgerichte naar een ordergerichte eindassemblage. FAS wordt ingevoerd om ordergericht de eindassemblage los van het MPS (Master Production Schedule) te kunnen plannen. De implementatie van de productconfigurator geschiedt omwille van ondersteuning van verkoop bij het uitvoeren van een beschikbaarheidstoets bij orderacceptatie. Er is immers geen voorraad eindproduct maar alleen maar voorraad halffabrikaat.
Andere meer overkoepelende projecten zijn het definiëren en realiseren van managementinformatie en het inrichten c.q. verbeteren van de internecontrolefunctie.

De doorlooptijd van de optimalisatiefase varieert per deelproject en is sterk afhankelijk van de complexiteit van de door te voeren organisatorische veranderingen tijdens de optimalisatie. De projectorganisatie is in tegenstelling tot de basisfase sterk bezet vanuit de organisatie zelf. Optimalisatie kan immers worden gekarakteriseerd als een organisatieveranderingsproject. Betrokkenheid en actieve deelname van de organisatie zelf is voor succes een voorwaarde. Vaak wordt de optimalisatiefase ondersteund door organisatie- c.q. processpecialisten met kennis van het onderhavige systeem.

Belangrijke activiteiten bij de start van de optimalisatiefase zijn het reviewen van de resultaten van de basisfase en het hernieuwd (opvolging van vooronderzoek) vaststellen wat de inhoud van de optimalisatiefase moet zijn (zie ook figuur 2). Het reviewen van de basisfase is nodig aangezien basis- en optimalisatiefase afhankelijk van elkaar zijn (de optimalisatiefase 'borduurt voort' op het resultaat van de basisfase). Het is belangrijk een volledigheids- en kwaliteitscontrole op de geïmplementeerde basisfunctionaliteiten uit te voeren, om een goed uitgangspunt voor optimalisatie te creëren.

Tevens wordt definitief vastgesteld wat allemaal geïmplementeerd zal worden tijdens de optimalisatiefase. Dit was reeds gedefinieerd in de basisfase. Echter, gedurende deze fase kunnen wijzigingen in opgestelde specificaties zijn opgetreden of




*Figuur 2. Activiteitenoverzicht voor de optimalisatiefase.*

additionele behoeften zijn ontstaan. Bekeken dient te worden in hoeverre dergelijke systeem'wijzigingen' nog kunnen worden meegenomen tijdens de optimalisatiefase. Vervolgens kunnen de deelprojecten worden vastgesteld en uitgevoerd.

Een interessante vraag is: 'Wanneer stopt de optimalisatiefase?' Bedrijfsprocessen kunnen immers continu worden verbeterd en ook komen er regelmatig nieuwe pakketmodules op de markt. Optimalisatie stopt in feite dan ook nooit! Het is vanuit projectbeheersingsoogpunt wel zaak duidelijk af te bakenen wat nu wanneer dient te worden opgeleverd met welke baten. Daarom wordt optimalisatie in 'golven' uitgevoerd. Per 'golf' is sprake van een behapbaar project voor de organisatie met een duidelijk en beheersbaar projectplan.

Interessant blijft nu de vraag hoe de verdeling van functionaliteit over de twee deelfasen precies vorm kan worden gegeven. Met andere woorden: waar ligt de grens tussen basis- en optimalisatiefase?

## GRENSBEPALING TUSSEN DE TWEE IMPLEMENTATIEFASEN

Bij de start van een implementatieproject vindt allereerst een *voorstudie* plaats.

Eén van de stappen die gedurende deze voorstudie wordt uitgevoerd, is het zo volledig mogelijk definiëren van de functies die moeten worden geïmplementeerd. Indien pas tijdens de optimalisatiefase blijkt dat extra en/of andere functionaliteiten gewenst zijn, kan dit gevolgen hebben. Deze functionaliteiten kunnen immers een bepaalde instelling in het pakket vereisen die achteraf niet zomaar aan te brengen is op een operationeel systeem (systeem is immers na de basisfase reeds operationeel).

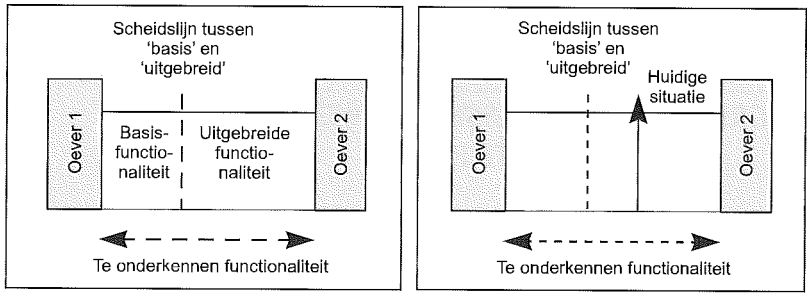
Bij het vaststellen van de te implementeren functionaliteiten voor de basis- en optimalisatiefase dient rekening te worden gehouden met het veranderingsvermogen van de organisatie. De impact van te implementeren functionaliteiten kan worden in-

Indien een industrieel bedrijf managementinformatie wil genereren met behulp van het nieuwe standaardpakket ten behoeve van het bepalen van de omzet van de tien grootste klanten per regio, dient bij het parametriseren van het systeem rekening te worden gehouden met het aanleggen van deze regio's. Indien *pas tijdens de optimalisatie* blijkt dat deze managementinformatie gewenst is, kan dit betekenen dat de structuur zoals deze reeds in het pakket in de basisfase is verwezenlijkt, dient te worden gewijzigd. Al ingevoerde orders moeten worden voorzien van de link naar regio's. Dit betekent een ongewenste, extra conversieslag.

*Voorbeeld 5. Belang van een adequaat ingerichte voorstudie.*

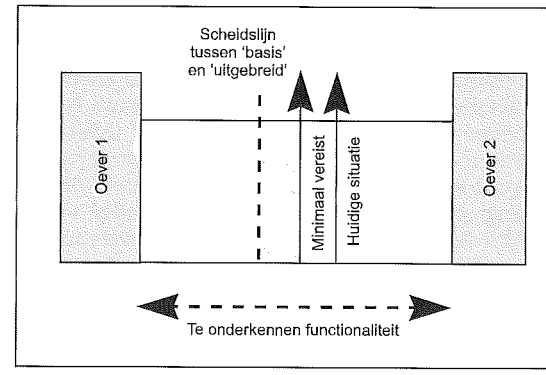
geschat met behulp van een zogenaamde behoeftescan. De behoeftescan meet de mate van veranderingsvermogen die benodigd is voor het adequaat doorvoeren van de vereiste aanpassingen in de organisatie. Naast de behoeftescan dient ook een zogenaamde vermogensscan te worden uitgevoerd. De vermogensscan meet het veranderingsvermogen waarover de organisatie beschikt. Tezamen bepalen beide scans de haalbaarheid van de organisatorische veranderingen die gepaard gaan met de implementatie van bepaalde functionaliteiten; de gevolgde techniek wordt dan ook haalbaarheidsscan genoemd. Met behulp van deze scan wordt bepaald of de organisatie de organisatorische veranderingen aankan die het gevolg zijn van implementatie van de functionaliteiten die de organisatie aan het einde van de optimalisatiefase in het systeem verwezenlijkt wil zien.

Vervolgens wordt een opsplitsing gemaakt tussen te implementeren functionaliteiten in de basis- en optimalisatiefase. Essentieel hierbij is om na te gaan wat de organisatie op dit moment aan geautomatiseerde ondersteuning heeft. Een eventuele mismatch tussen normaal te implementeren basisfunctionaliteiten in de basisfase en bestaande automatisering (huidige situatie) kan immers onaanvaardbaar zijn (zie figuur 3).




*Figuur 3. Verdeling in basis- en uitgebreide functionaliteiten.*

Indien in de huidige situatie functionaliteit aanwezig is die normaliter niet in de basisfase wordt geïmplementeerd (bijvoorbeeld MPS), zal allereerst worden nagegaan wat het belang is van deze functionaliteit voor het functioneren van de organisatie. Via vragenlijsten worden de kwaliteit, de mate van gebruik en het belang vastgesteld. Bovendien wordt vastgesteld of de uitgebreide functionaliteit wellicht eenvoudig naast de nieuw te implementeren functionaliteit kan bestaan (door koppeling van het stand-alonesysteem aan het nieuwe systeem). Doel van deze exercitie is om na te gaan welke functionaliteit voor een organisatie 'minimaal vereist' is. Deze dient vervolgens te worden meegenomen bij de implementatie van functionaliteiten in de basisfase (zie figuur 4).




*Figuur 4. De huidige situatie en de minimaal vereiste functionaliteiten.*

Een organisatie maakt in de huidige situatie reeds gebruik van 'eindige capaciteitsplanning'. Dergelijke functionaliteit wordt normaliter niet als basisfunctionaliteit gekenmerkt.
Idealiter zou de opsplitsing tussen basis- en optimalisatiefase worden geplaatst op de scheidslijn tussen basis- en uitgebreide functionaliteit. Eindige capaciteitsplanning zou dan in de optimalisatiefase worden geïmplementeerd. Echter, eindige capaciteitsplanning is een functionaliteit die voor dit bedrijf minimaal vereist is; het bedrijf kan zonder de eindige planningsfunctionaliteiten het productieproces niet adequaat ondersteunen. In dergelijke gevallen dient er een specifieke oplossing te worden gevonden.

Situatie 1:
Indien *eindige planning in de huidige situatie uitgevoerd wordt via een apart stand-aloneschedulingpakket,* kan tijdens de basisfase een koppeling worden gelegd tussen het nieuwe pakket en de bestaande eindige planningssoftware. De eindige planningsmodule van het *nieuwe* pakket wordt in de basisfase nog niet ingezet noch vindt optimalisatie van het gebruik van eindige planning plaats, maar toch hoeft het bedrijf het niet zonder eindige planning te stellen.

Situatie 2:
Mocht eindige planning in de huidige situatie echter via maatwerk 'ingebakken' zitten in het oude systeem, dan zit er niets anders op dan 'eindige planning' mee te nemen in de basisfase (met consequenties voor de doorlooptijd).

*Voorbeeld 6.*
*Minimale vereisten bij opsplitsing.*

## TOEGEVOEGDE WAARDE GEFASEERDE PAKKETIMPLEMENTATIEAANPAK

De gefaseerde implementatieaanpak levert, mits goed uitgevoerd en bewaakt, de volgende voordelen op:

- Na het afronden van de basisfase kan de organisatie reeds gebruikmaken van het nieuwe systeem; 'hands-on-experience' kan worden opgedaan hetgeen de overgang naar implementatie van complexe en uitgebreide functionaliteiten vereenvoudigt.

- De stapsgewijze verandering: verandering in samenhang met intensieve begeleiding tijdens de optimalisatiefase leidt veelal tot beter doorgevoerde en geaccepteerde veranderingen. Het pakket wordt intensiever gebruikt en nieuwe concepten gaan daadwerkelijk werken.

- De opsplitsing in een basis- en een optimalisatiefase en binnen de optimalisatiefase in vaak zelfstandige deelprojecten leidt tot een beter beheersbaar project. De totale kosten en doorlooptijd lijken in eerste instantie vaak hoger en langer. Na afloop blijkt het tegendeel. Het doel, zo kort mogelijke terugverdientijd met maximalisatie van de baten, wordt beter gerealiseerd.

## LITERATUUR

[Beek95] J.J. van Beek, W. Boogaard en J.J.B. van den Oever, *AO en standaardpakketten: integratie verhoogt de kans op een succesvolle selectie en implementatie*, Compact 1995/4.

[Tias96] E.P.R. van Vroenhoven, *Implementation Pitfalls*, Graduation Ceremony BIK/MIM, juni 1996.

[Vroe96] E.P.R. van Vroenhoven, *De rol van EDP Auditing bij aanschaf standaardpakketten*, Nieuwsbrief BIKMag/Bestuurlijke Informatiekunde, juni 1996.

[Zwar96] C. de Zwart, *Implementatie logistieke pakketten is een gigantische klus: Heliview onderzocht stand van zaken logistieke automatisering*, PolyTechnisch tijdschrift, mei 1996.

*Drs. M.A.A. Jongen*
*Is sinds 1995 werkzaam bij KPMG EDP Auditors. Momenteel is hij bezig met de postdoctorale EDP-auditopleiding aan de Katholieke Universiteit Brabant. Hij maakt deel uit van een business unit die zich volledig richt op selectie en implementatie van standaardpakketten. In diverse projecten is hij betrokken geweest bij het selecteren en implementeren van geïntegreerde standaardpakketten.*

*R.L.M. Essers*
*Studeert Bestuurlijke informatiekunde aan de Katholieke Universiteit Brabant in Tilburg en is momenteel als stagiair verbonden aan KMPG EDP Auditors. Hij voert onderzoek uit naar diverse methoden van implementatie van geïntegreerde standaardpakketten.*

*Drs. E.P.R. van Vroenhoven RE RA*
*Is werkzaam als senior manager bij KPMG EDP Auditors. Hij geeft leiding aan de business unit Pakketten, welke zich richt op pakketselectie van ERP-pakketten. Tevens is hij als docent verbonden aan de postdoctorale opleiding EDP-auditing van het Tilburgs Instituut voor Academische Studies (TIAS).*

# IT-trends en ERP-pakketwaarde

Drs. M.J.H. Giesbers RE,
dr. G.J. van der Pijl RE en
drs. E.P.R. van Vroenhoven RE RA

**Objectoriëntatie en workflow management komen in veel varianten voor. De toegevoegde waarde die objectoriëntatie en workflow management bieden in ERP-pakketten is afhankelijk van de variant van de trend in het pakket. Het is bij een pakketselectie dus van belang om de verschillen in toegevoegde waarde tussen de varianten te weten.**

## INLEIDING

De praktijk laat zien dat vier op de vijf bedrijven besluiten om bij het aanschaffen van nieuwe software te kiezen voor een standaard-softwarepakket ([Boer95]). Bij tekstverwerkers en spreadsheets ligt dit percentage bijna op honderd procent. De populariteit van standaardpakketten heeft een aantal redenen.

Het in eigen huis ontwikkelen van software brengt voor veel bedrijven een te hoog risico met zich mee. Het uitbesteden van de ontwikkeling van software is goedkoper en minder gecompliceerd. Daarnaast wordt de kwaliteit van de standaardsoftwarepakketten steeds beter en bieden standaardpakketten door parametrisering steeds meer de mogelijkheid om het pakket aan te passen aan de specifieke eisen en wensen van de organisatie. Een andere reden is dat nagenoeg alle functionele gebieden in een organisatie door standaardpakketten worden afgedekt: financiën, personeel en salaris, inkoop, verkoop, productiebesturing, etc.

Standaardpakketten die onder andere de gebieden logistieke besturing en financiën afdekken, worden *Enterprise Resource Planning*-pakketten (of kort: ERP-pakketten) genoemd. Bekende voorbeelden van ERP-pakketten zijn SAP R/3 van SAP, Triton en Baan IV van Baan, BPCS van SSA en MFG/PRO van Largotim.

Om het pakket te onderscheiden van de concurrenten prijzen leveranciers van ERP-pakketten de producten vaak aan door gebruik te maken van dure en veelbelovende (technische) trends. Trends, zoals grafische user interface (GUI), objectoriëntatie (OO), client/server (C/S), groupware, electronic data interchange (EDI), open systemen, workflow management (WFM), worden gebruikt zonder dat ze een duidelijk beeld geven wat (voor de gebruiker) de toegevoegde waarde is. Is de toegevoegde waarde bijvoorbeeld functioneel van aard? Zit de toegevoegde waarde in extra toepassingsmogelijkheden?

Bovenstaande vragen worden in dit artikel beantwoord. Om de veelheid aan trends in te perken worden de trends objectoriëntatie en workflow management behandeld.

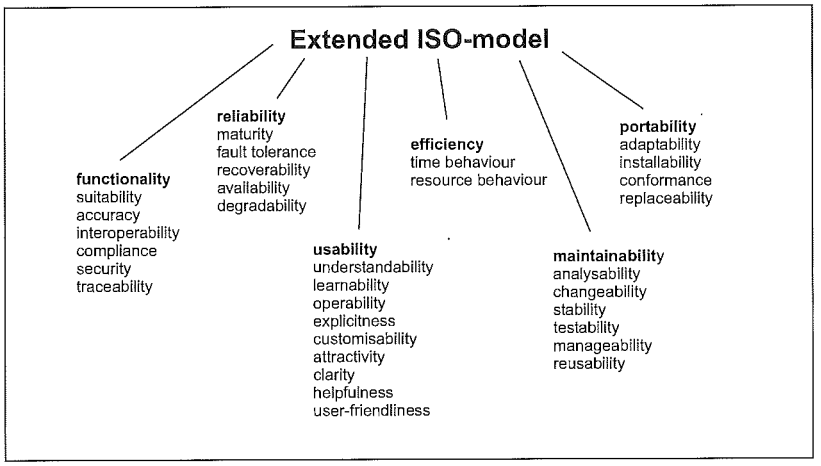
## TOEGEVOEGDE WAARDE

Het analyseren van de toegevoegde waarde van een trend is een complexe aangelegenheid. Om de analyse te structureren wordt gebruikgemaakt van het Extended ISO-model ([Zeis96]). Het model onderscheidt verschillende kwaliteitsaspecten in een softwarepakket. Vertaald in het Nederlands zijn deze kwaliteitsaspecten:

1. functionaliteit;
2. betrouwbaarheid;
3. bruikbaarheid;
4. efficiency;
5. onderhoudbaarheid;
6. overdraagbaarheid.

Elk van deze kwaliteitsaspecten kan worden onderverdeeld naar subaspecten. In figuur 1 is het totale Extended ISO-model weergegeven.

Indien een trend toegevoegde waarde levert aan de kwaliteit van het softwareproduct, zal de trend toegevoegde waarde moeten geven aan minimaal één van de aspecten van het model. Bij de analyse van de toegevoegde waarde van een trend wordt dus geanalyseerd of een trend een substantiële verbetering van een aspect laat zien.




*Figuur 1. Extended ISO-model van het SERC. (Bron: Van Zeist e.a., 1996.)*

## OBJECTORIËNTATIE

Bij objectoriëntatie kan een aantal belangrijke begrippen/aspecten worden onderscheiden:

- object;
- attribuut;
- methode;
- klasse en overerving;
- communicatie (object brokering/Object Management Architecture).

Het objectoriëntatieparadigma kent als uitgangspunt dat de wereld of werkelijkheid beschreven kan worden als een verzameling van losstaande objecten die met elkaar communiceren ([Schu94]). Het belangrijkste begrip bij objectoriëntatie is het begrip *object*. De definitie van een object is:

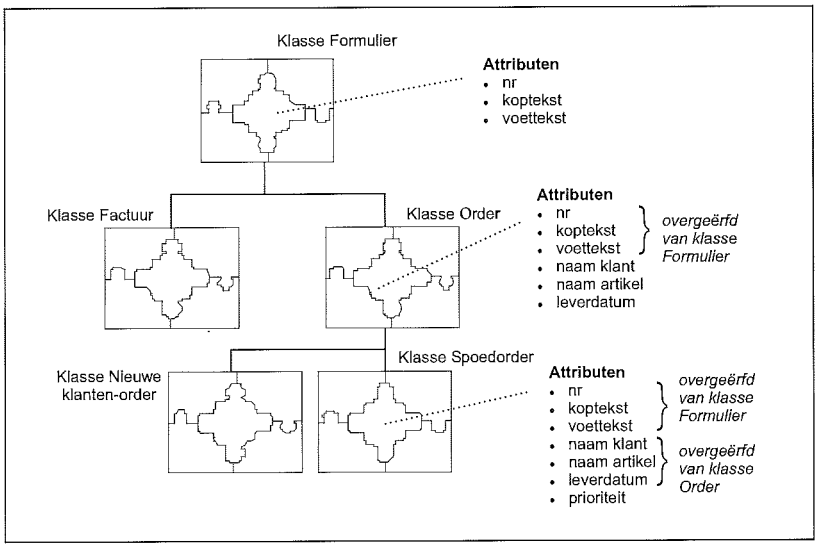
Een object is een samenvoeging van gerelateerde attributen en methoden om acties op die attributen te kunnen uitvoeren. De attributen representeren het statische gedeelte van een object. De methoden bepalen het gedrag, en daarmee het dynamische gedeelte, van het object.

De *attributen* van een object zijn de karakteristieken van een object. Voorbeelden van attributen van een object Order_1 zijn *nummer, naam artikel, naam klant* en *leverdatum*. Voorbeelden van methoden van een object Order_1 zijn *printen* en *wijzigen leverdatum*. De *methoden* vormen als het ware een schild of capsule rond de attributen van het object. Handelingen op de attributen van het object kunnen *alleen door de methoden* van dat object worden uitgevoerd. Door dit alleenrecht bepalen de methoden van een object het gedrag van dat object.

Andere belangrijke begrippen zijn *klasse* en het daarmee samenhangende begrip *overerving*. Het begrip *klasse* is gedefinieerd als een verzameling van objecten met gemeenschappelijke attributen en methoden. In figuur 2 is de klasse *Order* een voorbeeld van een klasse met objecten welke allemaal dezelfde attributen (nr, koptekst, etc.) en methoden bezitten. (De waarden voor de verschillende attributen zijn natuurlijk niet hetzelfde!).
Indien binnen de groep van objecten van de klasse Order een subgroep van objecten kan worden aangewezen die alle dezelfde attributen bezitten, kan een subklasse worden gemaakt. In de subklasse Spoedorder zitten bijvoorbeeld alle objecten die als extra attribuut het attribuut Prioriteit hebben. De klasse Spoedorder erft als subklasse van de klasse Order alle attributen en methoden van de klasse Order; alleen het attribuut Prioriteit hoeft te worden toegevoegd.

**Communicatie (object brokering/ Object Management Architecture)**

Een belangrijk aspect van objectoriëntatie is de manier van communiceren. Deze manier verschilt van de manier van communiceren in niet-objectgeoriënteerde omgevingen. Bij niet-objectgeoriënteerde omgevingen is de meest gebruikte manier die door middel van Remote Procedure Calls (RPC's) ([KPMG96]). Communiceren door middel van RPC




*Figuur 2. Klasse. (Bron: Giesbers e.a., 1996.)*

is enigszins vergelijkbaar met communiceren in een objectgeoriënteerde omgeving. In plaats van een procedure aan te roepen, wordt in een objectgeoriënteerde omgeving een object 'gevraagd' om een bepaalde methode uit te voeren. Dit verzoek aan het object verloopt door middel van (gestandaardiseerde) berichten.

De Object Management Group, een organisatie waarvan alle op objectoriëntatie actieve organisaties lid zijn, heeft vanwege het belang van een wereldwijde standaardisatie van berichten de Object Management Architecture (OMA) in het leven geroepen. De OMA beschrijft de architectuur voor communicatie in objectgeoriënteerde omgevingen. Deze OMA onderscheidt vier onderdelen:
1. application objects;
2. common facilities;
3. object services;
4. object request broker.

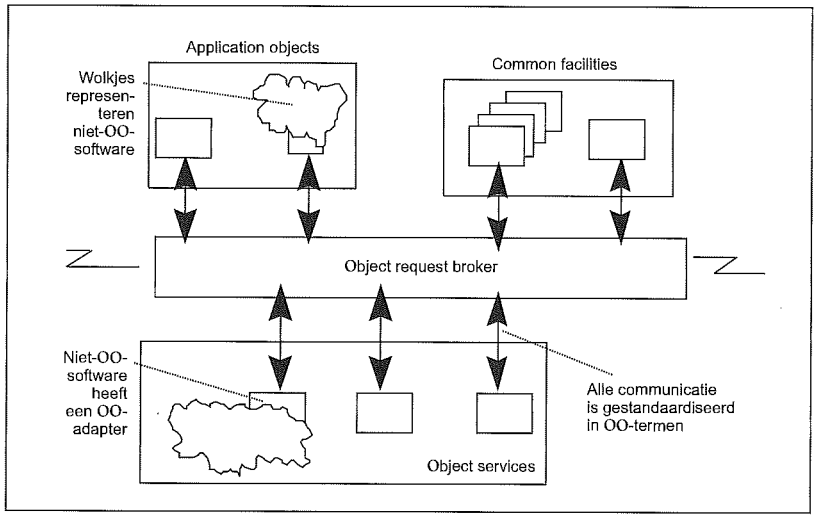
Hieronder worden de vier onderdelen kort uiteengezet.

*Application objects*
Onder application objects (AO) worden de softwarepakketten verstaan. Voorbeelden van applicaties zijn spreadsheets, tekstverwerkers, ERP-pakketten, en dergelijke. Indien deze softwarepakketten niet via berichten communiceren, bestaat de mogelijkheid om met een interface een laag rondom de applicatie te 'leggen' waardoor de omgeving de applicatie als object ziet en deze via berichten kan benaderen.

*Common facilities*
Common facilities is een set van generieke applicatiefuncties. Voorbeelden van dergelijke functies zijn *Systeem management* en *Task management* ([Data95]).

*Object services (OS)*
Deze categorie bevat functies die fundamenteel zijn voor applicaties gebaseerd op de objecttechnologie. Met andere woorden, object services zijn voor object computing wat directorystructuren en directoryservices, naamconventies, en andere belangrijke services zijn voor procedureel programmeren en conventioneel systeemmanagement. Voorbeelden van object services zijn *Naming* ten behoeve van een eenduidige en unieke benaming van objecten en *Query* ten behoeve van manipulatieoperaties voor het verzamelen, invoegen, verwijderen, etc. van informatie van objecten ([Data95]).

*Figuur 3. OMG's Object Management Architecture. (Bron: Datapro, 1995.)*




*Object request broker (ORB)*
Het belangrijkste onderdeel in een objectgeoriënteerde architectuur is de object request broker (ORB). Een ORB bezit een aantal belangrijke functionaliteiten, zoals bijvoorbeeld de mogelijkheid om ORB's op verschillende platformen met elkaar te laten communiceren en het bijhouden welke methoden een object bezit ([Mart92]). De ORB is als het ware het bloed in een objectgeoriënteerde omgeving.

In figuur 3 zijn de onderdelen en hun samenhang weergegeven.

Naast de OMA heeft de OMG ook voor de functionaliteiten van een ORB standaarden opgesteld. Het resultaat hiervan is de Common Object Request Broker Architecture (CORBA). De bekendste voorbeelden van CORBA-compliant ORB's ([Schr94]) zijn de ObjectBroker van Digital Equipment, de Distributed Object Management Facility (DOMF) van Hewlett Packard, de Distributed Objects Everywhere (DOE) van Sunsoft, en het Distributed System Object Model (DSOM) van IBM.

**Objectoriëntatie bij ERP-pakketten**

In softwarepakketten kunnen grofweg drie varianten in objectoriëntatie worden onderscheiden:
1. objectgeoriënteerd;
2. object based;
3. geen objecten.

Objectgeoriënteerde software is software die is opgebouwd uit objecten. Voorwaarde is dat de objecten communiceren door middel van berichten, wat het gebruik van een ORB vereist. De objecten zelf dienen ook gebouwd te zijn door een objectgeoriënteerde taal of tool en niet enkel op basis van een omhullende laag tot object te zijn verheven.

Kenmerk van object based is dat de software eveneens in 'objecten'/modules is verdeeld. De objecten kunnen communiceren op een objectgeoriënteerde manier met behulp van een ORB, maar bijvoorbeeld ook door gebruik te maken van Remote Procedure Calls (RPC's). Ook de mate van modulariteit kan sterk verschillen. Zo kan een module bijvoorbeeld een financieel pakket zijn, maar kan een module ook de functie voorstellen voor het invoeren van een order.

Bij de laatste variant kunnen geen losstaande modules/'objecten' worden onderkend. De software is één brok waarbij dus geen sprake is van communicatie gebaseerd op objectgeoriënteerde principes binnen de software. Een voorbeeld van dergelijke software is software geschreven in de programmeertaal BASIC.

Uit onderzoek is gebleken dat op dit moment zich onder de bekende ERP-pakketten nog geen pakket-

ten bevinden die objectgeoriënteerd zijn, met andere woorden die een ORB bezitten en in een objectgeoriënteerde taal zijn gebouwd. De toegevoegde waarde die objectoriëntatie kan geven, dient dan ook in een toekomstig perspectief te worden gezien.

**Toegevoegde waarde van objectoriëntatie**

In tabel 1 is voor de verschillende varianten van objectoriëntatie aangegeven op welke aspecten zij toegevoegde waarde leveren.

*Onderhoudbaarheid*
Een belangrijk voordeel van objectoriëntatie op het aspect onderhoudbaarheid is de *beheersbaarheid*. Indien bij een aantal objecten bijvoorbeeld een attribuut moet worden veranderd, kan door de klassenhiërarchie van aanwezige objecten bij objectoriëntatie in één keer deze aanpassing voor alle objecten worden gemaakt door in de hogere klasse van de objecten deze verandering door te voeren. Deze toegevoegde waarde geldt alleen voor de variant objectoriëntatie. Bij de andere varianten moet elk 'object' afzonderlijk worden aangepast!

Een ander voordeel is een verbetering van het aspect *aanpasbaarheid*. Een kenmerk van de grondslag van het onderkennen van onafhankelijke objecten is dat een object zonder problemen uit zijn omgeving kan worden losgemaakt. Bovendien kan het object zonder problemen in aangepaste vorm weer terug worden geplaatst. Er hoeft geen rekening te worden gehouden met bijvoorbeeld extra koppelingen binnen de software. Een voorbeeld op het gebied van versiebeheer kan dit aspect verduidelijken. Een pakket bestaat uit een object Order met de methode 'Is order op voorraad' en een object Voorraad. Gebruik van objecten geeft nu de mogelijkheid om aanpassingen in het object Voorraad te kunnen doen zonder dat dat consequenties heeft voor de methode van het object Order. Deze toegevoegde waarde geldt met name voor de objectgeoriënteerde variant, maar zal eveneens in beperkte mate aanwezig zijn bij object based indien hierbij een grote mate van standaardisatie dan wel conventies met betrekking tot modules wordt gehanteerd.

Bovenstaande voordelen zijn voor de huidige ERP-pakketten van cruciaal belang. Door de vergaande integratie en uitbreiding van functionaliteit binnen deze pakketten wordt de complexiteit van ERP-pakketten danig vergroot. Objectoriëntatie geeft de mogelijkheid om ERP-pakketten beter onderhoudbaar te maken. Deze complexiteitsbeheersing is ook een gevolg van de grondslag van objectoriëntatie in het onderkennen van kleine, *onafhankelijke* stukjes software (objecten) ([Schu94]). Deze grondslag zorgt dat ieder stukje software kan worden bestudeerd zonder dat hierbij met invloeden van de omgeving rekening hoeft te worden gehouden. Dit voordeel geldt voor objectoriëntatie, maar ook voor object based software waar de opmaak van 'objecten' sterk gestandaardiseerd is.

Een min of meer losstaand voordeel binnen de onderhoudbaarheid is het voordeel van *hergebruik*. Indien software objectgeoriënteerd is, kunnen objecten of gedeelten van objecten worden hergebruikt. Onterecht wordt dit voordeel vaak uniek aan objectoriëntatie toegewezen. Doordat bij object based eveneens 'objecten' worden onderkend, kan ook hergebruik van 'objecten' of delen van 'objecten' plaatsvinden. Er zijn hele bibliotheken met kant-en-klare software en mechanismen beschikbaar ([Auto96]) die dezelfde mate van hergebruik leveren als objectoriëntatie.

| Aspect | OO | Object based | Geen 'objecten' |
|---|---|---|---|
| Functionaliteit | | | |
| Betrouwbaarheid | + | + | |
| Bruikbaarheid | | | |
| Efficiency | – | | |
| Onderhoudbaarheid | ++ | + | |
| Overdraagbaarheid | + | | |

*Tabel 1. Toegevoegde waarde van de varianten van objectoriëntatie.*

*Betrouwbaarheid*
Indien een ORB aanwezig is en dus door berichten tussen de objecten wordt gecommuniceerd, wordt de betrouwbaarheid door objectoriëntatie vergroot. Objecten hebben een schil van methoden om zich. Een object zal alleen een actie uitvoeren indien een aanvraag op de juiste manier aan een methode wordt gesteld. Bij een foute manier van aanvragen zal het object geen actie ondernemen. Op deze manier zal een fout zich niet verder kunnen verspreiden. Software wordt door objectoriëntatie dus stabieler.

Een ander voordeel van betrouwbaarheid is het deelaspect beschikbaarheid. Objecten kunnen zonder veel moeite worden toegewezen aan een platform ([Haak96]). Indien de gebruiker bijvoorbeeld op elk moment de beschikking moet hebben over bepaalde informatie kan het desbetreffende object aan de PC van de gebruiker worden toegewezen.

*Overdraagbaarheid*
Het laatste aspect dat als voordeel van objectoriëntatie naar voren komt, is het subaspect *vervangbaarheid*. Door de gestandaardiseerde manier van communiceren van objecten (door middel van de CORBA-architectuur) kan elk object worden vervangen door een soortgelijk object. Het maakt dus niet uit of een module van pakket X of van pakket Y wordt gebruikt. De organisatie kan kiezen voor het pakket dat het beste voldoet aan de eisen en wensen die aan de module worden gesteld.

*Efficiency*
Uit de praktijk blijkt dat het aantal berichten dat voor het uitvoeren van een computerhandeling nodig is, sterk kan oplopen. Door deze toenemende berichtencommunicatie verslechtert de efficiency van het softwarepakket zowel op het gebied van de responsietijd c.q. transactietijd als op het gebied van de middelenbeslaglegging.

*Kanttekening*
Het opvallendste aspect bij objectoriëntatie is dat objectoriëntatie geen nieuwe functionaliteiten creëert die niet door gebruik van modules (object based) zouden kunnen worden gerealiseerd ([Gies96]). De reden hiervoor is dat objectoriëntatie

en modulair programmeren hetzelfde paradigma van modules/objecten als basis hebben.

## WORKFLOW MANAGEMENT

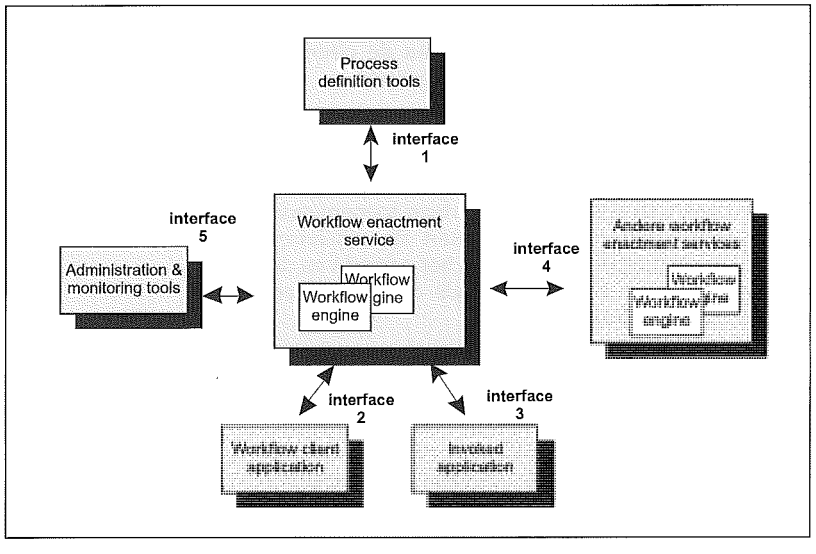
De tweede trend die in dit artikel wordt behandeld, is workflow management. WFM is het managen van de workflow, waarbij gebruik wordt gemaakt van een workflow-managementsysteem (WFMS). Definities voor beide begrippen zijn:

Workflow is the computerized facilitation or automation of a business process, in whole or part ([WFMC94]).
Workflow-managementsysteem (WFMS): A system that completely defines, manages and executes 'workflows' through the execution of software whose orde of execution is driven by a computer representation of the workflow logic ([WFMC94]).

Bovenstaande definities zijn van de Workflow Management Coalition (WFMC). De WFMC is ontstaan uit een gezamenlijke interesse van mensen met verschillende achtergronden. De Workflow Management Coalition is geïnitieerd als orgaan dat zich bezighoudt met standaardisatie rond workflow management. Op dit moment zijn alle belangrijke leveranciers op het gebied van WFM lid van de WFMC. De coalitie heeft verscheidene standaarden opgesteld, bijvoorbeeld ten aanzien van componenten en interfaces van een WFMS.

In een WFMS kunnen drie verschillende onderdelen worden onderscheiden, te weten:
1. componenten;
2. interfaces;
3. architectuur.

*Componenten workflow-managementsysteem*
De softwarecomponenten van een workflow-managementsysteem zijn:
a. het definition tool;
b. de workflow enactment service;
c. de worklist handler;
d. het administration & control tool.




*Figuur 4. Workflow Management Coalition Reference Model. (Bron: WFMC, 1994)*

Het *definition tool* wordt gebruikt om de procesbeschrijving in een voor de computer begrijpbare vorm weer te geven. De data die nodig zijn om de workflow uit te voeren, zitten verpakt in de proces definition data. Veel definition tools geven ook de mogelijkheid om activiteiten in de workflow aan mensen in de organisatie toe te wijzen.

De *workflow enactment service* is de samenvoeging van de *workflow engine* en de voor de uitvoering benodigde data, zoals de definition data, workflow control data en de organigram data. Binnen de workflow enactment service is de *workflow engine* de 'motor'. Activiteiten van deze engine zijn bijvoorbeeld het interpreteren van de procesbeschrijving, het controleren van de workflow en het opstarten van externe applicaties.

De *worklist handler* stuurt de interactie tussen de workflowparticipanten (gebruikers) en de workflow enactment service. Daar waar de workflow enactment service bepaalt welke activiteiten dienen te worden uitgevoerd, bepaalt de handler wie die activiteiten gaat uitvoeren. De handler is zodoende nauw verbonden met de user interface. De activiteiten verschillen per worklist handler en kunnen variëren van het plaatsen van een uit te voeren activiteit in een TO DO-lijst tot het toewijzen van uit te voeren activiteiten aan gebruikers en het balanceren van activiteiten tussen de gebruikers.

De laatste component is het *administration & control tool*. Dit tool geeft het workflow-managementsysteem extra mogelijkheden op het gebied van het verzamelen van informatie, bijvoorbeeld over de doorlooptijd of voortgang van de workflow. Veelal bieden deze tools mogelijkheden om de informatie grafisch weer te geven.

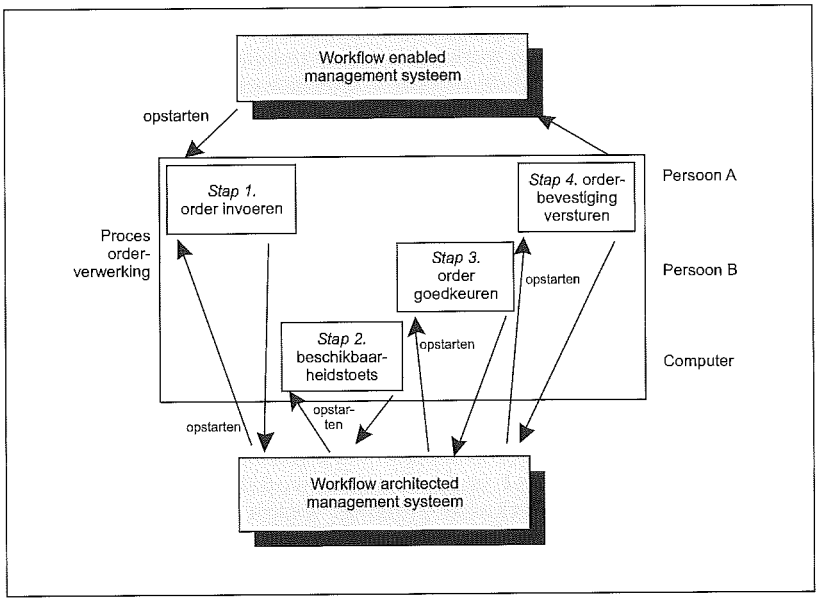
*Interfaces workflow-managementsysteem*
Het bekendste product van de Workflow Management Coalition is het *Workflow Reference Model*. In dit model heeft de coalition uiteengezet welke interfaces in een workflow-managementsysteem kunnen worden onderkend. De aanwezigheid van componenten, zoals een administration & control tool of een definition tool, veronderstelt reeds de aanwezigheid van bepaalde interfaces. Het totaal van onderkende interfaces is ([WFMC94]):
1. *Interface 1*: koppeling met definition tools;
2. *Interface 2*: koppeling met workflow client applications (zoals bijvoorbeeld de worklist handler);
3. *Interface 3*: koppeling met invoked applications (zoals bijvoorbeeld WordPerfect of financiële software);
4. *Interface 4*: koppeling met andere workflow enactment services;
5. *Interface 5*: koppeling met administration & monitoring tools.

In figuur 4 zijn de verschillende interfaces en de onderlinge relaties met de verschillende componenten weergegeven.

*Architectuur workflow-managementsysteem*
Het workflow-managementsysteem kan in twee architecturen voorkomen: de workflow management *enabled* architectuur en workflow manage-

ment *architected* architectuur ([Smar96]). Het verschil zit in het niveau waarop de workflow kan worden gestuurd. Workflow enabled systemen kunnen alleen modules of submodules aanroepen. Workflow architected systemen geven de mogelijkheid om op iedere actie in de workflow invloed uit te oefenen. Een voorbeeld kan het verschil verduidelijken.

In figuur 5 is het proces Orderverwerking weergegeven. Het proces kent vier deelstappen die door de personen A en B en de computer worden uitgevoerd. Een workflow enabled management systeem kan alleen het proces Orderverwerking opstarten en zal na afloop van het proces het 'stokje' weer terugkrijgen. Een workflow architected management systeem biedt daarentegen ook de mogelijkheid om de deelstappen in het proces te sturen. Stel: de organisatie voert de nieuwe regel in dat een order van een bepaalde grootte door persoon C dient te worden goedgekeurd: Deze stap hoeft in een architected WFMS slechts in de workflow-definitie te worden ingevoerd en kan zodoende snel worden doorgevoerd. Bij een enabled WFMS kan deze extra stap alleen door maatwerk worden gerealiseerd.




*Figuur 5. Workflow enabled versus workflow architected. (Bron: Giesbers e.a., 1996.)*

**Workflow management bij ERP-pakketten**

De hamvraag is welke componenten, interfaces en/of welke architectuur aanwezig moeten zijn, wil een ERP-pakket als workflow-managementsysteem kunnen worden aangemerkt. Bij een WFMS dienen vier onderdelen aanwezig te zijn ([Gies96]):
1. een definition tool;
2. een workflow enactment service;
3. een worklist handler;
4. interfaces voor koppelingen met applicaties.

Interfaces voor koppelingen (interface 3 en interface 4) is een eis omdat bij ERP-pakketten het workflowsysteem vaak met bestaande software, zoals bijvoorbeeld financiële software, moet kunnen 'samenwerken'. De architectuur heeft geen invloed op de vraag of een systeem een workflow-managementsysteem is. Het onderscheid in architectuur dient echter wel te worden gemaakt, omdat de architecturen een verschil in de toegevoegde waarde hebben.
Uit de componenten, interfaces en architectuur kunnen zes in de praktijk voorkomende varianten van ERP-pakketten worden samengesteld. In tabel 2 zijn de verschillende varianten weergegeven alsmede de onderdelen waaruit ze bestaan.

Op de markt zijn veel ERP-pakketten aanwezig die workflow management bieden. Er zijn echter ook pakketten die zeggen workflow management aan te bieden, maar niet de onderdelen bezitten die als minimale voorwaarde voor workflow management gelden.

De pakketten die reeds jaren bestaan, zullen nood-

| | Aanwezige onderdelen | | | | |
|---|---|---|---|---|---|
| **Varianten** | *Definition tool* | *Workflow enactment service* | *Koppelingen applicaties* | *Worklist handler* | *Administr. & control tool* |
| Basis enabled workflow systeem | x | x | x | | |
| Basis enabled workflow systeem met werkverdeling | x | x | x | x | |
| Enabled workflow systeem met werkverdeling en control | x | x | x | x | x |
| Basis architected workflow systeem | x | x | x | | |
| Basis architected workflow systeem met werkverdeling | x | x | x | x | |
| Architected workflow systeem met werkverdeling en control | x | x | x | x | x |

*Tabel 2. Variantenmodel workflow-managementsysteem. (Bron: Giesbers e.a., 1996.)*

gedwongen workflow management realiseren op een workflow enabled manier. De reden hiervoor is dat de workflow-managementfunctionaliteit rondom de reeds bestaande modules dient te worden gebouwd. De pakketten die nog relatief nieuw zijn, hebben de kans gekregen om workflow management in de basis van het pakket in te bouwen. Deze architectuur creëert de mogelijkheid workflow tot in de kleinste stap te sturen.

**Toegevoegde waarde van workflow management**

In tabel 3 is voor de verschillende varianten weergegeven welke toegevoegde waarde zij leveren.

*Functionaliteit*
Door workflow management wordt de accuraatheid vergroot omdat workflow management een werkwijze afdwingt waardoor de gebruiker minder fouten kan maken. Dit voordeel is bij alle varianten te onderkennen. Een voorbeeld is het melden van een te lage voorraad voor een artikel en het automatisch op het scherm laten verschijnen van een bestelopdracht voor dat artikel.

Ander voordeel bij het aspect functionaliteit is de mogelijkheid om bottlenecks in de workflow te signaleren en op te lossen. Indien een persoon te veel werk in zijn TO DO-lijst heeft of indien een persoon ziek is, kan dit worden gesignaleerd en kan het werk worden herverdeeld. Een voorwaarde is dat een administration & control tool in combinatie met een worklist handler aanwezig is.

Een ander voordeel op het gebied van de functionaliteit is de mogelijkheid om extra informatie over de workflow te geven. Een WFMS kan bijvoorbeeld informatie verschaffen over doorlooptijden van pickopdrachten van de afgelopen maanden.

Nog een ander voordeel dat een WFMS biedt, is het gebruik van triggers. De gebruiker kan hierdoor op bepaalde tijdstippen of aspecten worden gewezen. Voorbeelden bij het orderacceptatieproces zijn triggers bij tijdslimieten bij offertes/orders en triggers voor het versturen van een brief naar een klant of het bellen van een klant.

*Betrouwbaarheid*
Een ander voordeel van workflow management geldt ten aanzien van de betrouwbaarheid. Indien het workflow-managementsysteem een worklist handler bezit, kan het werkblad van de gebruiker optimaal worden ingericht. Het workflow-managementsysteem zou eventueel al voor de gebruiker de programma's kunnen opstarten. Het deelaspect *beschikbaarheid* van de software op de momenten dat de software nodig is, wordt hierdoor vergroot. Dit voordeel geldt voor alle WFMS waar een worklist handler aanwezig is.

*Bruikbaarheid*
Workflow management bewijst zijn meerwaarde ook op het gebied van de bruikbaarheid. Doordat het werkaanbod voor de gebruiker optimaal kan worden ingericht, wordt de benodigde inspanning van de gebruiker danig gereduceerd.

Daarnaast biedt workflow management met een worklist handler vaak de mogelijkheid om de user interface in te richten naar de wensen van de gebruiker. Hierbij kan gebruik worden gemaakt van TO DO-lijsten.

*Onderhoudbaarheid*
Bij de workflow management enabled architectuur zijn de workflow-managementaspecten ondergebracht in een apart informatiesysteem (de workflow-managementmodule). Doordat deze module min of meer losstaat, zal hij alleen zijn workflow-managementactiviteiten kunnen uitvoeren indien koppelingen worden gelegd vanuit de workflow-managementmodule met de andere systemen/modules, zoals bijvoorbeeld de financiële module. Deze koppelingen zorgen ervoor dat de *analyseerbaarheid* wordt verkleind. De extra koppelingen zijn immers extra verbanden in een toch al ingewikkeld ERP-pakket. Hierdoor zullen ook de aanpasbaarheid en de beheersbaarheid verslechteren.

*Overdraagbaarheid*
Door de workflow-managementmodule bij de enabled architectuur wordt ook de overdraagbaarheid verslechterd. De extra workflow-managementschil rondom de bestaande modules/systemen is verantwoordelijk voor het feit dat extra aanpassingsinspanning is benodigd indien de software naar een ander platform wordt overgedragen. Een ander nadeel van de benodigde koppelingen is dat het moeilijker is de workflow-managementmodule te vervangen.

*Kanttekening*
Indien sprake is van een workflow management architected architectuur zullen bovenstaande nadelen op het gebied van onderhoudbaarheid en overdraagbaarheid in mindere mate aanwezig zijn. De negatieve aspecten zijn bij een workflow management architected architectuur dus minder groot

*Tabel 3. Toegevoegde waarde van de varianten van workflow management.*

| *Aspect* | *Enabled WFMS* | *Enabled + werkverdeling* | *Enab. + werkverdeling + control* | *Architected WFMS* | *Architected + werkverdeling* | *Arch. + werkverdeling + control* |
|---|---|---|---|---|---|---|
| Functionaliteit | + | + | + | + | + | + |
| Betrouwbaarheid | | + | + | | + | + |
| Bruikbaarheid | | + | + | | + | + |
| Efficiency | | | | | | |
| Onderhoudbaarheid | – | – | – | +/– | +/– | +/– |
| Overdraagbaarheid | – | – | – | +/– | +/– | +/– |

dan bij een workflow management enabled architectuur.

In de literatuur ([Witt95]) wordt nog een aantal bedreigingen onderkend. Deze bedreigingen zijn meer van organisatorische aard en zijn:
- weerstand tegen verandering in werkzaamheden;
- de automatisering van werkprocessen kan uitmonden in sterk gereduceerde taakinhoud;
- automatisering legt de creativiteit van medewerkers aan banden;
- het big-brother-is-watching-you-effect;
- inbreng van de gebruiker op cruciale momenten kan worden weggeautomatiseerd.

## CONCLUSIE

In het artikel is naar voren gekomen dat de toegevoegde waarde van *objectoriëntatie* vergeleken met de varianten object based en 'geen objecten' met name bij het aspect onderhoudbaarheid ligt.

Deze verbeterde onderhoudbaarheid is voor ERP-pakketten een cruciaal aspect. Door de vergaande integratie worden de pakketten steeds complexer. Alleen indien de complexiteit binnen de perken blijft en de onderhoudbaarheid verbeterd wordt, kunnen deze ERP-pakketten nog beheersbaar blijven. Objectoriëntatie kan hierin voorzien.

Op dit moment zijn nog geen ERP-pakketten aanwezig die objectgeoriënteerd zijn. Binnen enkele jaren zijn die er wel en zal het belang van objectoriëntatie naar voren komen.

De toegevoegde waarde van *workflow management* ligt met name op het gebied van de functionaliteit. Daarnaast biedt workflow management bij de aanwezigheid van een worklist handler en een administration & control tool toegevoegde waarde op de aspecten betrouwbaarheid en bruikbaarheid.

In het artikel is echter ook naar voren gekomen dat workflow management nadelen kent op de aspecten onderhoudbaarheid en overdraagbaarheid, en dat dit tevens op het organisatorische vlak geldt.

Belangrijk bij workflow management is dat de organisatie dient na te gaan welke toegevoegde waarde ze uit het WFMS wil halen. Deze toegevoegde waarde stelt voorwaarden aan de onderdelen die aanwezig dienen te zijn in het ERP-pakket. Bij de pakketselectie dient de aanwezigheid van die onderdelen te worden nagegaan.

**Slotopmerking**

De essentie is om bij een pakketselectie na te gaan of het ERP-pakket objectgeoriënteerd is of workflow-managementfunctionaliteiten bezit, alsmede welke variant van de trend het pakket herbergt. Bovendien dient te worden vastgesteld of het ERP-pakket de toegevoegde waarde kan bieden die de organisatie eist. In dit artikel is voor de verschillende varianten van objectoriëntatie en workflow management besproken welke toegevoegde waarde zij de organisatie kunnen bieden.

## LITERATUUR


[Auto96] Redactie Automatisering Gids, *UML verenigt het beste van drie modelleermethoden*, Automatisering Gids, 27 september 1996.

[Boer95] J. de Boer en J.A.M. Donkers, *Informatieplanning en standaardpakketten*, Compact 1995/4.

[Data95] Datapro, *Distributed Systems: Concepts & Trends: Object Management Architecture*, McGraw Hill, July 1995.

[Gies96] M.J.H. Giesbers, G. van der Pijl en E. van Vroenhoven, *Object oriëntatie, workflow management en client/server onder vuur genomen*, afstudeerscriptie Katholieke Universiteit Brabant, 20 december 1996.

[Haak96] K. Haakma en K. Untersalmberger, *Fundament in veranderende omgeving: Voordelen client/server en object oriëntatie verenigd*, Computable, 19 april 1996, blz. 25-27.

[KPMG96] KPMG Amstelveen, *Open IT-architecturen*, proef cursusmateriaal, mei 1996.

[Mart92] J. Martin en J.J. Odell, *Object-oriented analysis and design*, Prentice-Hall, 1992.

[Schr94] J.J. Schreuder, *CORBA-objecten geïmplementeerd: Op de weg naar een object georiënteerde infrastructuur*, PC+, 31 maart 1994, blz. 13-17.

[Schu94] D. Schuyl-Laros en G. van Roekel, *Object oriëntatie: definitie en samenhang van begrippen uit het object georiënteerde domein*, Databaseclub NGI, Amsterdam 1994.

[Smar96] Dun & Bradstreet Software, *Smartstreàm for Distributed Enterprise: Eliminating Boudaries Through Workflow*, Dun & Bradstreet Software, 1996.

[WFMC94] Workflow Management Coalition, *The Workflow Reference Model: The Workflow Management Coalition Specification*, Document Number TC00-1003, Draft 1.0, 10 November 1994.

[Witt95] D.J.P. Witte, *Soepel met de voeten in de klei: Verschil in bedrijfsprocessen rechtvaardigt eigen workflow management*, Informatie, jaargang 37, nr. 10, 1995, blz. 590-597.

[Zeis96] B. van Zeist, P. Hendriks, R. Paulussen en J. Trienekens, *Kwaliteit van softwareproducten; praktijkervaringen met een kwaliteitsmodel*, Kluwer Bedrijfswetenschappen, 1996.



*Drs. M.J.H. Giesbers RE*
*Is werkzaam als EDP-auditor bij KPMG EDP Auditors. Hij heeft onderzoek gedaan naar objectoriëntatie, workflow management en client/server bij ERP-pakketten. Daarnaast maakt hij sinds 1996 deel uit van de business unit Pakketten, welke zich richt op pakketselecties van ERP-pakketten.*

*Dr. G.J. van der Pijl RE*
*Is werkzaam bij de vakgroep Bestuurlijke Informatiekunde & Accountancy van de Katholieke Universiteit Brabant. Hij is tevens Director of Study van de postdoctorale opleiding EDP-auditing van het Tilburgs Instituut voor Academische Studies (TIAS).*

*Drs. E.P.R. van Vroenhoven RE RA*
*Is werkzaam als senior manager bij KPMG EDP Auditors. Hij geeft leiding aan de business unit Pakketten, welke zich richt op pakketselectie van ERP-pakketten. Tevens is hij als docent verbonden aan de postdoctorale opleiding EDP-auditing van het Tilburgs Instituut voor Academische Studies (TIAS).*

# Pakketmededeling: de vlag moet de lading dekken

Drs. H.E. Sijbring RE RA

**Een pakketmededeling vormt de schriftelijke rapportage van een audit op één of meer kwaliteitsaspecten van standaardpakketten. Antwoord wordt gegeven op de vraag welke zekerheid het maatschappelijk verkeer kan en mag ontlenen aan de mededeling, afgegeven door een EDP-auditor, als uitkomst van een audit die gericht is op de certificering van een standaardpakket. Teneinde deze vraag te beantwoorden is een vergelijking gemaakt tussen de accountantsverklaring en een pakketmededeling. Op basis van deze vergelijking wordt een aantal aanbevelingen geformuleerd voor de vorm, formulering en inhoud van een pakketmededeling.**

## INLEIDING

In het enorme aanbod van standaardpakketten op de Nederlandse en internationale markt is het voor een softwareleverancier niet eenvoudig zich te onderscheiden met betrekking tot zijn product. Hierdoor is met name het fenomeen 'certificering van standaardpakketten' ontstaan. Door certificering van zijn product heeft de leverancier een belangrijk instrument gekregen om zich duidelijker van zijn concurrenten te onderscheiden.

Ook aan de vraagzijde blijken steeds meer bedrijven bij de selectie van een pakket zich mede te laten leiden door de vraag of het pakket wel of niet is gecertificeerd. De potentiële gebruiker tracht enige zekerheid te verkrijgen omtrent de kwaliteit van op de markt beschikbare producten.

De marktpartijen (vragers en aanbieders) bepalen de waarde van het proces van certificering. Certificeren is geen doel op zich, maar een hulpmiddel om afnemers te beschermen tegen slechte kwaliteit, respectievelijk aan te geven dat producten en diensten voldoen aan de eisen die essentieel zijn voor het gebruik ervan.

In dit artikel zal worden ingegaan op de volgende vragen:
- Wat is het belang van deze afgegeven pakketmededelingen voor het maatschappelijk verkeer?
- Is een verwachtingskloof tussen de gebruiker van de pakketmededeling en degene die een pakketmededeling heeft afgegeven, waar te nemen?
- Indien deze verwachtingskloof aanwezig blijkt te zijn, is het dan mogelijk deze kloof te verkleinen door standaardisatie van de inhoud en de vorm van deze mededelingen?

Voor de beantwoording van deze vragen zal eerst worden ingegaan op de productaudit; het beoordelen van de kwaliteit van een standaardpakket.

Vervolgens wordt ingegaan op de betekenis en de inhoud van de mededeling die het oordeel bevat van onderzoek gericht op één of meer kwaliteitsaspecten van een standaardpakket; de pakketmededeling. Besproken wordt of het mogelijk is door standaardisatie van deze mededeling het ontstaan van een verwachtingskloof tussen degene die de audit uitvoert en de gebruikers van de mededeling te voorkomen of te beperken. Hierbij worden aanbevelingen gegeven om het risico van het ontstaan van een verwachtingskloof tussen de EDP-auditor en de gebruikers van de mededeling te voorkomen.

Aansluitend is een voorstel opgenomen voor de standaardisatie van een pakketmededeling afgegeven door een EDP-auditor. In de laatste paragraaf worden de conclusies weergegeven.

Ten slotte zijn voorbeeldteksten opgenomen voor oordelen over één of meer kwaliteitsaspecten van een standaardpakket.

## BEGRIPPEN EN SCOPE-AFBAKENING

Allereerst zullen enkele begrippen worden gedefinieerd.
Voor certificering worden in de literatuur verschillende definities gegeven, waaronder:

Certificatie omvat alle activiteiten op grond waarvan een onafhankelijke instantie kenbaar maakt dat een gerechtvaardigd vertrouwen bestaat dat een duidelijk omschreven onderwerp van certificatie in overeenstemming is met een bepaalde norm of met een ander eisenstellend element ([Praa93]).

Het toepassen van een vastgelegde methodiek door een onpartijdige instelling met het doel:
- te kunnen vaststellen of producten, processen of diensten voldoen aan alle eisen volgens bepaalde normen of andere technische specificaties en
- een zodanig toezicht uit te oefenen op de leverancier dat wordt bewerkstelligd dat aan deze eisen bij voortduring wordt voldaan ([Init86]).

Centraal staat in de definities dat certificering een uitspraak betreft naar aanleiding van het toetsen aan normen. Certificering dient de potentiële gebruiker de zekerheid te geven dat de producten, de diensten en de kwaliteitssystemen voldoen aan de gestelde eisen. Een belangrijke voorwaarde daartoe is dat een onpartijdige instelling vaststelt dat aan de gestelde eisen wordt voldaan en toezicht houdt op het voortduren daarvan.

Uit de definities komt naar voren dat verschillende categorieën objecten onderwerp kunnen vormen van certificering. Door de Raad voor Certificatie is de volgende onderverdeling aangebracht:
1. product en dienst;
2. processen;
3. kwaliteitssysteem.

Productcertificatie betreft de keuring van producten/diensten, waarbij de kwaliteit van de producten/diensten aan de hand van vooraf gestelde eisen wordt vastgesteld.

Procescertificatie is gebaseerd op een regelmatige beoordeling van maatregelen en middelen die worden aangewend om te bereiken dat het proces beheerst verloopt, zodat verwacht mag worden dat het eindresultaat aan de eisen voldoet.

Kwaliteitssysteemcertificatie is gericht op het keuren van een kwaliteitssysteem aan de hand van normen betreffende kwaliteitswaarborging. Een kwaliteitssysteem is te omschrijven als een stelsel vastgelegde bedrijfskundige procedures en regels dat ten doel heeft te verzekeren dat een product, proces of dienst aan gestelde eisen voldoet.

Het beoordelen van één of meer kwaliteitsaspecten van standaardpakketten is een voorbeeld van een productaudit. Het object van beoordeling is niet het ontwikkelproces, maar het eindproduct van het ontwikkelproces: het standaardpakket. Proces- en kwaliteitsaudits vallen dan ook buiten de scope van dit artikel. Slechts beperkt zal worden ingegaan op de onderzoekswijze en de gehanteerde normen.

Software is globaal onder te verdelen in besturings- en toepassingsprogrammatuur. In dit artikel wordt uitsluitend ingegaan op toepassingsprogrammatuur. In het vervolg zal de toepassingsprogrammatuur worden aangeduid met standaardpakket.

Onder het maatschappelijk verkeer worden in dit artikel alle personen en organisaties verstaan die gebruikmaken van de diensten van de EDP-auditor. Dit kan zowel de opdrachtgever zijn als degene die gebruikmaakt van de producten opgeleverd door de EDP-auditor. Certificeren en beoordelen worden in dit artikel beschouwd als synoniemen en zullen in het vervolg naast elkaar worden gebruikt.

## FASEN IN DE UITVOERING VAN EEN PRODUCTAUDIT

Bij het uitvoeren van een productaudit kunnen de volgende fasen worden onderscheiden:
1. opdrachtverstrekking;
2. vaststelling scope van de audit;
3. planning en uitvoering;
4. oordeelsvorming en rapportage.

Elke fase wordt hieronder kort behandeld.

## OPDRACHTVERSTREKKING

Bij de opdrachtverstrekking zijn onder meer de opdrachtgever en de opdrachtnemer van belang.

De opdracht tot het uitvoeren van een productaudit kan afkomstig zijn van verschillende delen van het maatschappelijk verkeer die ieder hun eigen beweegredenen hebben (zie tabel 1).

In de praktijk blijken diverse instanties te kunnen optreden als opdrachtnemer:
- openbare accountantskantoren;
- openbare EDP-auditorskantoren;
- interne auditorsdiensten;
- overheidsdiensten als de EDP-audit Pool;
- software- en adviesbureaus, keuringsinstanties en dergelijke.

Uit deze opsomming blijkt ook de verzameling van opdrachtnemers te bestaan uit een 'kleurrijk' gezelschap.

Het uitvoeren van een EDP-audit en het uitspreken van een oordeel vereist een bepaalde deskundigheid. Aangezien een auditor in de eerste plaats een controlerende taak vervult zal hij primair het controlevak moeten beheersen, dat wil zeggen kennis moeten hebben van:
- de methoden en middelen van de controle *en*
- de vaardigheid in hun toepassing *en*
- het object van controle.

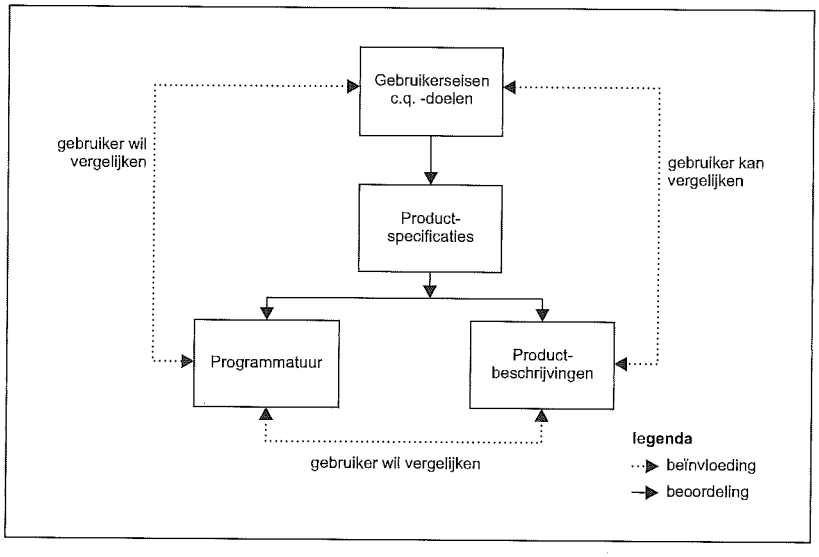
| Opdrachtgevers | Reden |
|---|---|
| – leverancier | – het verkrijgen of het behouden van concurrentievoorsprong;<br>– het beperken van de mogelijke productaansprakelijkheid door klanten; |
| – potentiële koper | – het verkrijgen van zekerheid omtrent bepaalde kwaliteitsaspecten in een pakketselectietraject; |
| – management van de organisatie | – het verkrijgen van zekerheid omtrent mogelijkheden tot het adequaat beheersen van de automatisering binnen de organisatie in verband met bijvoorbeeld de logische toegangsbeveiliging, de kosten van software en de hoogte van de onderhoudskosten ten opzichte van de aanschafkosten;<br>– een wettelijke verplichting; |
| – accountant | – door het gebruik van de mededeling wordt de totale controleopdracht doelmatiger en dus goedkoper;<br>– zonder het vormen van een oordeel over de betrouwbaarheid en de continuïteit van het informatiesysteem is het niet mogelijk tot een oordeel over de jaarrekening te komen;<br>– het verlenen van adviezen om marketingtechnische redenen;<br>– een wettelijke verplichting; |
| – overheid | – het maatschappelijk belang; |
| – brancheorganisatie | – het imago van de branche;<br>– een wettelijke verplichting. |

*Tabel 1. Een aantal opdrachtgevers van uit te voeren productaudits en hun beweegredenen.*

De kennis van het product dat het object vormt van de beoordeling zal veelal bij alle hiervoor genoemde opdrachtnemers wel aanwezig zijn. Van cruciaal belang is echter in hoeverre de opdrachtnemer kennis heeft van de methoden en middelen van controle *en* de vaardigheid in de toepassing van deze methoden en middelen. De EDP-auditor kan worden geacht kennis te hebben van alle drie punten.

Het uitvoeren van een productaudit ten behoeve van derden vereist een onafhankelijke positie en een onpartijdigheid in het oordeel. De onpartijdigheid moet mede tot uitdrukking komen in de mondelinge en schriftelijke rapportage van de EDP-auditor. In het geval dat degene die een pakketmededeling afgeeft een Register EDP-auditor (RE) is, zijn voor de opdrachtgever en andere belanghebbenden garanties aanwezig omtrent zijn deskundigheid. Iemand kan uitsluitend Register EDP-auditor worden en blijven indien hij voldoet en blijft voldoen aan allerlei kwaliteitseisen die zijn gesteld door de beroepsorganisatie van Register EDP-auditors (NOREA).

*Figuur 1. Beoordelen op basis van productbeschrijving.*




## VASTSTELLEN SCOPE VAN DE AUDIT

De scope van een audit wordt bepaald door het onderzoeksobject, de kwaliteitsaspecten, de kwaliteitseisen en de diepgang waarmee het object wordt onderzocht.

### Onderzoeksobject

Bij de beoordeling van de kwaliteit van het standaardpakket als onderzoeksobject spelen de volgende vragen een rol:
- Welke uitgangspunten (ex-ante*productspecificaties*) vormden de basis voor de ontwikkeling van het standaardpakket?
- Wat is er van deze uitgangspunten in het standaardpakket terechtgekomen?
- Hoe zijn de productspecificaties onder woorden gebracht (*productbeschrijving*)?
- Welke *gebruikersdoelen* heeft de afnemer van het standaardpakket (specifieke *eisen* afnemer)?

In het voor de gebruiker gunstigste geval komen de productspecificaties, het standaardpakket, de productbeschrijving en zijn gebruikersdoelen met elkaar overeen.

Bij de beoordeling of een standaardpakket aan zijn specifieke wensen voldoet kan de gebruiker in het algemeen alleen afgaan op de productbeschrijving. Hij wil eigenlijk weten of het programma zelf aan de eisen voldoet. De waarde van beoordeling door een onafhankelijke derde ligt met name in de vaststelling dat de software, de productbeschrijving en de gebruikersdoelen met elkaar overeenkomen. Zo'n beoordeling impliceert dan een onderzoek naar de juiste weergave van ex-postspecificaties van de programmatuur in de productbeschrijving. De verschillende relaties zijn in figuur 1 weergegeven.

Omdat de productbeschrijving hierbij fungeert als referentiecriterium, zal een dergelijke beoordeling alleen toegevoegde waarde hebben als zo'n productbeschrijving aan bepaalde minimumeisen voldoet. Om voldoende houvast te bieden voor een beoordeling zal een antwoord moeten worden gegeven op de volgende vragen:
- Welke functies kent het programma?
- Met welke nauwkeurigheid worden functies uitgevoerd?
- Wat hebben storingen van andere systeemcomponenten voor gevolgen voor het goed functioneren van het programma?

- Op welke wijze wordt foutieve invoer c.q. verkeerd gebruik afgevangen of veroorzaakt dit een onvoorspelbaar gedrag dat niet van een normaal gedrag is te onderscheiden?
- Wat is de minimale machineconfiguratie waarop het programma werkt en wat is daarbij de verwerkingssnelheid c.q. responsietijd per relevante eenheid respectievelijk wat zijn daarbij de beperkingen in de prestaties van het programma?
- Is het programma op een eenvoudige wijze door de leverancier te onderhouden en zo ja, wat zijn daarvan de kosten voor de afnemer?
- Is het programma geschikt voor meerdere typen/merken apparatuur en wat zijn de eventuele kosten voor de afnemer bij verandering van apparatuur?

Wanneer is vastgesteld dat de productbeschrijving aan de minimumeisen voldoet, moet vervolgens in detail worden nagegaan of het product (het standaardpakket) zelf overeenstemt met de productbeschrijving.

**Kwaliteitsaspecten**

Een productaudit richt zich op het beoordelen van één of meer kwaliteitsaspecten van een bepaald object.

Over de exacte betekenis van het begrip kwaliteit bestaat zowel bij de auditors als bij het maatschappelijk verkeer geen consensus. Kocks verwoordt dit als volgt: 'het zal de lezer duidelijk zijn dat wanneer het om het begrip kwaliteit gaat een semantische jungle wordt betreden. Het begrip kwaliteit is net een kameleon waarvan de huidskleur zich aanpast aan de omgeving. De huidskleur past zich aan aan de context.' ([Kock93]). Uit dit citaat valt af te leiden dat de uiteindelijke inhoud van het begrip kwaliteit wordt bepaald door de context waarin het wordt gebruikt.

Door het begrip kwaliteit te ontbinden in een aantal *kwaliteitsaspecten* is de eerste stap gezet in de concretisering van dit begrip. Zoals uit de definitie blijkt, richt een EDP-audit zich op het beoordelen van één of meer kwaliteitsaspecten van een bepaald object. Ook over de te onderscheiden kwaliteitsaspecten en de betekenis van elk kwaliteitsaspect bestaat zowel bij de auditors als bij het maatschappelijk verkeer geen consensus.

Een definitie van kwaliteitsaspecten kan alleen maar door het koppelen van een kwaliteitsaspect aan een object. Eigenlijk dient het begrip kwaliteit afzonderlijk voor elke combinatie van een aspect en een object te worden gedefinieerd. Toch is niet elke combinatie zinvol.

In NIVRA-geschrift 53 ([NIVR89]) is een additionele relatie gelegd tussen het kwaliteitsaspect en de doelgroep waarvoor het oordeel van de EDP-auditor bestemd is. Deze afstemming dient per object te worden gemaakt omdat, zoals hierboven is aangegeven, de inhoud van een kwaliteitsaspect per object kan verschillen. In tabel 2 is dit als voorbeeld voor het object Standaardpakket uitgewerkt. De 'x' geeft aan dat de doelgroep geïnteresseerd kan zijn in het kwaliteitsaspect en dat derhalve voor deze doelgroep de inhoud van dit aspect voor dit object dient te worden vastgesteld.

| | **Doelgroep** | | | |
|---|---|---|---|---|
| **Aspect** | *Management* | *Leverancier* | *Accountant* | *Branche-organisatie* |
| Effectiviteit | x | x | | x |
| Betrouwbaarheid | x | x | x | x |
| Vertrouwelijkheid | x | x | (x) | x |
| Continuïteit | x | x | (x) | x |
| Controleerbaarheid | x | x | x | x |
| Onderhoudbaarheid | x | x | | x |
| Gebruikers-vriendelijkheid | x | x | | x |
| Flexibiliteit | x | x | | x |
| Efficiëntie | x | x | | x |

*Tabel 2. Relatie tussen betekenis van het kwaliteitsaspect en de doelgroep voor het object Standaardpakket.*

NIVRA-geschrift 53 besteedt ten onrechte geen expliciete aandacht aan de relatie tussen kwaliteitsaspect en object.

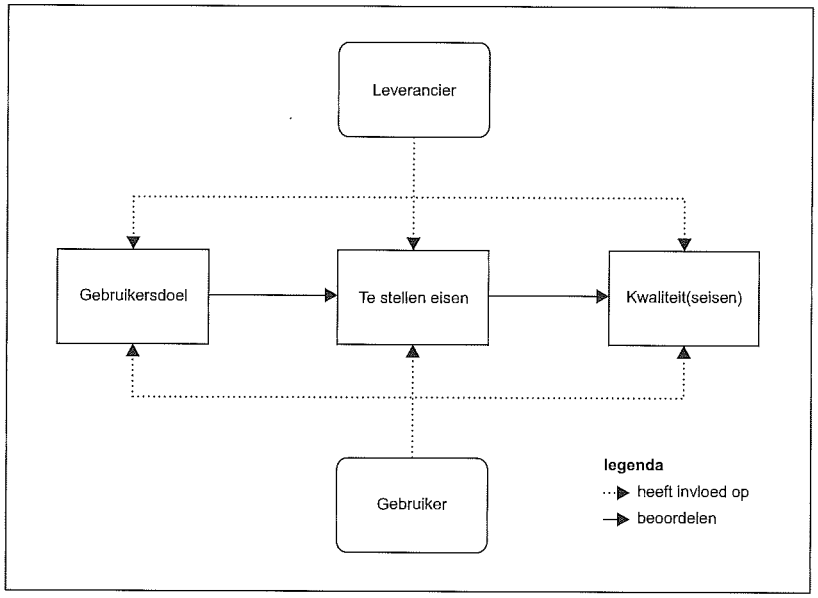
Bij elke beoordelingsopdracht van de kwaliteit van een standaardpakket dienen zowel vooraf bij de opdrachtaanvaarding als achteraf bij de rapportage het object en het (de) betrokken kwaliteitsaspect(en) expliciet te worden vastgelegd.

**Kwaliteitseisen**

In het algemeen is het doel dat met het object van de EDP-audit wordt beoogd, bepalend voor de hardheid van de norm die wordt opgelegd bij de oordeelsvorming en de diepgang van het onderzoek. Een oordeel bestaat altijd uit een vergelijking tussen het te beoordelen object en een norm. Deze normen kunnen afkomstig zijn uit de wet en jurisprudentie, algemeen aanvaarde geschriften (bijvoorbeeld NIVRA-geschriften), de wetenschap, de opdrachtgever en de auditor. De beoordeling zal bij een EDP-audit betrekking hebben op het beoordelen van kwaliteitsaspect(en) van het object ten opzichte van één of meer normen. De normen waaraan een standaardpakket kan worden getoetst, kunnen sterk uiteenlopen.

Om een product te kunnen beoordelen dienen expliciete eisen te worden geformuleerd voortvloeiend uit het gebruikersdoel. De opdrachtgever, de opdrachtnemer en gebruikers zullen tot overeenstemming moeten komen over de omschrijving van het gebruikersdoel van het standaardpakket. Op basis van deze definitie van het gebruikersdoel dient vervolgens consensus te worden bereikt over de te stellen eisen. Deze relatie is in figuur 2 afgebeeld.

Op dit moment is deze consensus nog niet bereikt en kan er ook nog geen sprake zijn van een verzameling algemeen aanvaarde normen voor pakketbeoordelingen. Als gevolg van het ontbreken van deze set moet noodzakelijkerwijs bij elk oordeel aangegeven worden aan welke normen het standaardpakket wordt getoetst.




*Figuur 2. Relaties in het ontwikkelproces van normen.*

**Diepgang**

Met diepgang wordt in dit verband bedoeld dat een onderzoek betrekking kan hebben op de opzet, de opzet en het bestaan dan wel de opzet en de werking van het programmapakket. De opzet heeft betrekking op het ontwerp van maatregelen, het bestaan betreft de daadwerkelijke uitvoering van de maatregelen op een bepaald moment en de werking is het bestaan gedurende een zekere periode.

In NIVRA-geschrift 53 is een aantal factoren genoemd die van invloed zijn op de diepgang van het onderzoek:
- de oogmerken van de opdrachtgever;
- het type oordeel dat de doelgroep verlangt;
- het beschikbare budget;
- de lengte van de onderzoeksperiode;
- de deskundigheid van degene die het onderzoek uitvoert;
- de arbeid benodigd voor het formuleren van normen.

Beperking van de diepgang van het onderzoek op grond van deze factoren is op zich geen bezwaar mits:
- de opdrachtgever hiermee akkoord gaat;
- geen wettelijke bepalingen of andere richtlijnen zich hiertegen verzetten (bijvoorbeeld gedrags- en beroepsregels zoals de GBR voor registeraccountants en de GBRE voor Register EDP-auditors);
- de consequenties in de rapportage zijn omschreven.

## PLANNING EN UITVOERING

De planningsfase omvat de gebruikelijke activiteiten bij het uitvoeren van een audit. Controletechnieken die bij het uitvoeren van een beoordeling van een standaardpakket worden toegepast zijn inlichtingen van de gecontroleerde, kennisnemen van de documentatie en directe waarnemingen.

Hoe verloopt nu de beoordeling van een standaardpakket? De volgende stappen zijn te onderscheiden:

a. Controle van de productbeschrijving
Nagegaan wordt of de productbeschrijving voldoet aan de norm (minimuminhoud) en of de beweringen in de productbeschrijving controleerbaar zijn.

b. Installatie
De installatieprocedure zoals opgegeven door de leverancier wordt uitgevoerd en op juistheid gecontroleerd.

c. Controle van de documentatie
Naast de productbeschrijving (zie a.) zal er nog meer documentatie zijn zoals een gebruikershandleiding. Gecontroleerd wordt of de documentatie consistent en volledig is en in overeenstemming is met de productbeschrijving.

d. Programmatest
Op grond van de documentatie en de te beoordelen kwaliteitsaspecten wordt een testplan opgesteld. De definitie van de aard en de omvang van de uit te voeren werkzaamheden wordt vastgelegd in een testscenario. De relevante grenswaarden die in de documentatie zijn vermeld, worden daarbij getest (bijvoorbeeld alle symbolen per record, maximale bestandsomvang). Tevens is er een test op robuustheid. Dit betekent dat bij iedere relevante invoerfunctie wordt nagegaan hoe het pakket reageert op het gebruik van de niet-gedefinieerde toetsen. Ten slotte wordt gecontroleerd of de juiste foutmeldingen worden gegeven in overeenstemming met het vermelde in de documentatie.

## OORDEELSVORMING EN RAPPORTAGE

Aan het eind van het proces van testen zal een oordeel dienen te worden gevormd. Degene die belast is met de beoordeling van het standaardpakket zal de uitkomsten van zijn onderzoek kenbaar moeten maken aan zijn opdrachtgever en eventuele andere doelgroepen. Veelal zal dit op een schriftelijke wijze gebeuren. Het rapport dient de volgende onderdelen te bevatten:
- het onderzoeksobject;
- de beoordeelde kwaliteitsaspecten;
- de normen waaraan het object wordt getoetst;
- de resultaten van de beoordeling;
- de pakketmededeling met het oordeel;
- eventuele aanbevelingen.

De vorm, de formulering en de inhoud van het oordeel wekken verwachtingen bij gebruikers van de pakketmededeling. De schriftelijke rapportage dient op een zodanige wijze te worden samengesteld dat de kans op interpretatieverschillen tussen de gebruikers van de mededeling en degene die de mededeling heeft afgegeven zo beperkt mogelijk wordt gehouden. De wijze waarop het oordeel wordt vormgegeven, dient binnen de grenzen van vaktechnische normen te worden afgestemd op degene die daarvan gebruikmaakt.

## FORMULERING, VORM EN INHOUD

Voor de EDP-auditor geldt dat hij aan het eind van het beoordelingsproces zich een oordeel dient te vormen over de mate waarin het standaardpakket voor elk te beoordelen kwaliteitsaspect voldoet aan de gestelde normen. De EDP-auditor zal vervolgens zijn oordeel kenbaar moeten maken aan de opdrachtgever. Veelal zal dit op een schriftelijke wijze gebeuren. Eerder is al aangegeven dat er een grote verscheidenheid is in opdrachtgevers. Elke opdrachtgever heeft zijn eigen beweegredenen en zal met het verstrekken van de opdracht de intentie hebben om één of meer delen van het maatschappelijk verkeer te bereiken. Tevens is opgemerkt dat voor het beoordelen van een product normen dienen te worden geformuleerd voortvloeiend uit het gebruikersdoel. Zo dienen de opdrachtgever, de opdrachtnemer en gebruikers tot overstemming te komen over de omschrijving van het gebruikersdoel van het standaardpakket. Het gebruikersdoel kan voor elke gebruikersgroep verschillen, hetgeen zal resulteren in een andere normenset.
Ook geldt dat het voor elk deel van het maatschappelijk verkeer duidelijk dient te zijn of het behoort tot de doelgroep waarvoor de schriftelijke rapportage met oordeel over de kwaliteit(saspecten) van het standaardpakket bestemd is dan wel waaraan die rapportage gericht is. Indien andere delen van het maatschappelijk verkeer, die niet behoren tot de doelgroep die de EDP-auditor voor ogen heeft, gebruikmaken van de pakketmededeling bestaat het gevaar dat zij de rapportage anders zullen interpreteren dan de EDP-auditor heeft bedoeld. Deze interpretatieverschillen kunnen leiden tot een verwachtingskloof tussen de EDP-auditor en dit deel van het maatschappelijk verkeer.

In deze paragraaf zal antwoord worden gegeven op de vraag: welke zekerheid kunnen en mogen de verschillende *delen* van het maatschappelijk verkeer die behoren tot de *doelgroep* waarvoor de mededeling bestemd is, ontlenen aan de mededeling, afgegeven door een EDP-auditor, als uitkomst van een audit die gericht is op de certificering van een standaardpakket?
Om deze vraag te kunnen beantwoorden wordt aansluiting gezocht bij de accountantsverklaring afgegeven bij een jaarrekening. Gekeken zal worden naar de overeenkomsten en verschillen tussen deze accountantsverklaring bij een jaarrekening en de mededelingen bij een standaardpakket. Ingegaan zal worden op de mogelijkheden die de strekking, de formulering en de inhoud van een mededeling bieden teneinde het risico op het ontstaan van een verwachtingskloof tussen de gebruikers van de mededeling en de EDP-auditor te minimaliseren.
Voor het aanduiden van de rapportage inclusief het oordeel over de kwaliteit(saspecten) van een standaardpakket zal in deze paragraaf de term *pakketmededeling* worden gebruikt.

## VERGELIJKING ACCOUNTANTSVERKLARING BIJ EEN JAARREKENING EN PAKKETMEDEDELING

De belangrijkste overeenkomsten en verschillen tussen de accountantsverklaring bij een jaarrekening en de mededelingen bij een standaardpakket worden weergegeven (tabel 3). De verschillen die van belang zijn voor het beantwoorden van de in de inleiding genoemde vragen zullen achtereenvolgens afzonderlijk worden behandeld.

### Object

Het object is afhankelijk van het doel van de audit.

*Accountantsverklaring*
Bij een accountantsverklaring afgegeven bij een jaarrekening bestaat het object uit de jaarrekening. In de loop van de tijd is maatschappelijke consensus bereikt over de vorm van de jaarrekening. Deze consensus is vastgelegd in de Richtlijnen voor de Jaarverslaggeving, die zijn opgesteld door de verschaffers, de gebruikers en de controleurs van de jaarrekening. Deze richtlijnen worden regelmatig onderhouden en aangevuld op grond van maat-

*Tabel 3. Overeenkomsten en verschillen tussen de accountantsverklaring bij een jaarrekening en pakketmededeling.*

| | *Verklaring afgegeven bij een jaarrekening* | *Mededeling afgegeven bij een standaardpakket* |
|---|---|---|
| *Soort audit* | product | product |
| *Object* | jaarrekening | software en/of documentatie |
| *Kwaliteitsaspect(en)* | getrouwheid | divers, waaronder bijvoorbeeld betrouwbaarheid |
| *Normen* | – Richtlijnen voor de Jaarverslaggeving<br>– Burgerlijk Wetboek 2 titel 9<br>– overige wettelijke bepalingen | gebruikersdoelen en -eisen |
| *Doelgroep* | meerdere delen van het maatschappelijk verkeer | één of meer delen van het maatschappelijk verkeer |
| *Verstrekker van de uitkomst van de audit* | registeraccountant c.q. certificerend accountant | geen wettelijke beperking; veelal een EDP-auditor |
| *Bewoording van het oordeel* | gedeeltelijk verplicht voorgeschreven in:<br>– GBR<br>– Richtlijnen voor de Accountantscontrole | geen voorgeschreven formuleringen |
| *Strekking van het oordeel* | verplicht voorgeschreven systematiek van strekkingen | geen voorgeschreven systematiek |
| *Wijze van oordeelsvorming* | materialiteit; kwantitatief | kwalitatief en mogelijk kwantitatief |
| *Wettelijk verplicht* | ja, indien binnen bepaalde criteria volgens Burgerlijk Wetboek 2 titel 9 | nee |

schappelijke ontwikkelingen en jurisprudentie. In de accountantsverklaring kan dan ook volstaan worden met een korte omschrijving van het object.

*Pakketmededeling*
Zoals reeds eerder in dit artikel aangegeven, kan het object van een pakketmededeling gevormd worden door documentatie (productbeschrijving) en/of door de software. In de pakketmededeling van de EDP-auditor dient duidelijk te worden aangegeven wat het object is van de audit: de documentatie, de software of de documentatie en de software. Daarnaast dient het object zodanig te worden omschreven dat duidelijk is welke documenten en/of modules zijn meegenomen in de beoordeling. Ook dient te worden aangegeven welke softwareversies zijn beoordeeld door vermelding van het versienummer en de datum. Overwogen kan worden om aan te geven welke modules niet zijn meegenomen in de beoordeling.

**Kwaliteitsaspecten**

Ook de kwaliteitsaspecten zijn afhankelijk van het auditdoel.

*Accountantsverklaring*
Reeds is aangegeven dat een kwaliteitsaspect alleen betekenis heeft door dit te koppelen aan een object. Bij de accountantsverklaring bij een jaarrekening is het te beoordelen kwaliteitsaspect steeds de getrouwheid van het object Jaarrekening. De getrouwheid van de jaarrekening is nader toegelicht in de Richtlijnen voor de Accountantscontrole, waarover in de accountantswereld voldoende duidelijkheid bestaat. Afgevraagd kan worden of er tussen de verschillende delen van het maatschappelijk verkeer die gebruikmaken van de accountantsverklaring voldoende consensus bestaat over de betekenis van het kwaliteitsaspect getrouwheid in relatie tot het object Jaarrekening. Het ontstaan van de verwachtingskloof tussen de accountant en delen van het maatschappelijk verkeer lijkt erop te wijzen dat dit niet het geval is.

*Van de termen 'verstandige leek' en 'maatschappelijk verkeer' van Limperg dient te worden afgestapt.*

*Pakketmededeling*
Bij pakketmededelingen kunnen de te beoordelen kwaliteitsaspecten steeds verschillen. Zowel bij de EDP-auditors als bij de gebruikers van de rapportage van de EDP-auditor bestaat geen consensus over de te onderscheiden kwaliteitsaspecten en de betekenis van elk kwaliteitsaspect in relatie tot een bepaald object. Gesteld kan worden dat wegens het ontbreken van deze consensus bij elke beoordeling van de kwaliteit van een standaardpakket zowel vooraf in de opdracht als achteraf in de rapportage de volgende punten dienen te worden opgenomen:
- een opsomming van de onderzochte kwaliteitsaspecten in relatie tot het object;
- een omschrijving van elk onderzocht kwaliteitsaspect in relatie tot het object.

**Normen**

De normen vloeien voort uit de doelstellingen van de audit.

*Accountantsverklaring*
Het NIVRA heeft omstreeks 1990 wijzigingen aangebracht in de systematiek en de formuleringen van de accountantsverklaringen teneinde een effectievere communicatie met de gebruikers 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 (Boek 2 BW titel 9). De normen voor het beoordelen van de getrouwheid van de jaarrekening zijn voor de accountant en de gebruikers van de jaarrekening voldoende geconcretiseerd in de vorm van wettelijke voorschriften en richtlijnen voor de jaarverslaggeving. In de accountantsverklaring kan daarom volstaan worden met een verwijzing naar deze wettelijke voorschriften en richtlijnen.

*Pakketmededeling*
Bij een pakketmededeling ontbreken algemeen aanvaarde normen. Om het object te kunnen beoordelen dienen expliciete eisen te worden geformuleerd, voortvloeiend uit het gebruikersdoel.
De opdrachtgever, de opdrachtnemer en gebruikers zullen tot overeenstemming moeten komen over de omschrijving van het gebruikersdoel van het standaardpakket. Op basis van deze definitie van het gebruikersdoel dient vervolgens consensus te worden bereikt over de te stellen eisen (de normen). De voor deze beoordeling geldende eisen dienen expliciet te worden omschreven zodat belanghebbenden kunnen vaststellen op basis van welke eisen de EDP-auditor tot zijn oordeel is gekomen. De gehanteerde normen dienen ingedeeld te worden per kwaliteitsaspect en indien mogelijk per module.

**Doelgroep**

Onder *doelgroep* worden in dit artikel verstaan één of meer delen van het maatschappelijk verkeer waarvoor de pakketmededeling is bestemd.

*Accountantsverklaring*
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'. Volgens de Vertrouwenstheorie van Limperg is het optreden als vertrouwensman van het maatschappelijk verkeer de hoofdfunctie van de accountant ([Sijbr96]). Limperg ziet de afnemer van het accountantsproduct, de verstandige leek, in slechts één bepaalde hoedanigheid. In de tijd van Limperg was er slechts

één belanghebbende bij de verslaggeving van de onderneming, namelijk de vermogensverschaffer. Onder invloed van de economische, sociale en technologische ontwikkelingen heeft de verstandige leek in de loop der tijd vele hoedanigheden gekregen en is de afnemer uitgegroeid tot een heterogeen samenstel van belanghebbenden (zoals: leveranciers, afnemers, werknemers, concurrenten, banken en de overheid). Door deze maatschappelijke ontwikkelingen kan niet meer volstaan worden met deze ongedifferentieerde termen. Voor het overbruggen van de verwachtingskloof tussen accountants aan de ene kant en de samenleving aan de andere kant dient te worden afgestapt van de termen 'verstandige leek' en 'maatschappelijk verkeer' zoals deze zijn gedefinieerd door Limperg ([Sijbr96]).

Een aantal recente wijzigingen in het verklaringenstelsel, zoals wijzigingen in de systematiek en de formuleringen van de accountantsverklaringen en het onderscheid tussen controle- en controleverwante opdrachten, heeft niet geleid tot het opnemen van een verwijzing naar of een omschrijving van het deel respectievelijk delen van het maatschappelijk verkeer waarvoor de verklaring is bestemd ([Sijbr96]).

*Pakketmededeling*

De samenstelling van de groep van belanghebbenden kan bij elke afgegeven pakketmededeling zeer verschillend zijn. Tevens bestaat er een grote verscheidenheid in de opdrachtgevers die elk hun eigen beweegredenen hebben voor het verstrekken van de opdracht. Deze beweegredenen zijn afhankelijk van de grootte en de samenstelling van de doelgroep die de opdrachtgever met de pakketmededeling wil bereiken.

Om te voorkomen dat de grootte en de samenstelling van de doelgroep die de opdrachtgever wil bereiken, afwijken van die welke de EDP-auditor voor ogen heeft, dienen in de fase van de opdrachtverstrekking en -aanvaarding duidelijke afspraken te worden gemaakt en vastgelegd. De opdracht dient in ieder geval de volgende elementen te bevatten:

- een duidelijke omschrijving van het object;
- een duidelijke omschrijving van de te beoordelen kwaliteitsaspecten in relatie tot het object;
- de reden waarom de opdrachtgever een beoordeling laat uitvoeren;
- een duidelijke omschrijving van de doelgroep die de opdrachtgever en de EDP-auditor gezamenlijk voor ogen hebben;
- de vorm en inhoud van de rapportage waarin de EDP-auditor de resultaten aan de doelgroep inclusief de opdrachtgever kenbaar zal maken;
- de wijze waarop de rapportage kenbaar zal worden gemaakt aan de doelgroep.

Kunnen de opdrachtgever en de EDP-auditor over één of meer van bovenstaande elementen geen overeenstemming bereiken dan kan de EDP-auditor de opdracht niet aanvaarden. Het gevaar van het ontstaan van een verwachtingskloof tussen de EDP-auditor en potentiële gebruikers van de door de EDP-auditor afgegeven pakketmededeling is dan te groot.

De samenstelling van de doelgroep dient de vorm, de formulering en de inhoud van de rapportage te bepalen om de interpretatieverschillen te vermijden. De doelgroep kan bestaan uit:

- delen van het maatschappelijk verkeer anders dan (uitsluitend) de opdrachtgever;
- uitsluitend de opdrachtgever.

In het geval dat de doelgroep bestaat uit andere delen van het maatschappelijk verkeer dan (uitsluitend) de opdrachtgever is niet altijd de mogelijkheid aanwezig dat elke belanghebbende, indien onduidelijkheden ontstaan naar aanleiding van rapportage van de EDP-auditor, terug kan vallen op de opdracht. De opdracht is immers veelal alleen in het bezit van de opdrachtgever. De elementen dienen daarom expliciet zowel in de opdracht als in de rapportage van de EDP-auditor te worden opgenomen. Aldus kan het ontstaan van een verwachtingskloof worden voorkomen respectievelijk het risico erop zoveel mogelijk worden beperkt.

Indien de doelgroep uitsluitend bestaat uit de opdrachtgever kan overwogen worden de rapportage vrij beperkt te houden omdat veel elementen reeds in de opdracht naar voren komen en de opdrachtgever immers altijd terug kan grijpen naar de opdracht indien van onduidelijkheden sprake is. De EDP-auditor zal dan voor een aantal elementen volstaan met het opnemen in de rapportage van een verwijzing naar de opdracht. De EDP-auditor dient in de rapportage aan te geven dat de rapportage alleen voor de opdrachtgever bestemd is en niet zonder expliciete toestemming van de auditor aan een derde mag worden verstrekt. Om alle misverstanden te vermijden is het echter aan te bevelen dat de elementen ook expliciet in de rapportage van de EDP-auditor zijn opgenomen.

Afhankelijk van de grootte en de samenstelling van de doelgroep (automatiseringsdeskundige, algemeen management, gebruiker van pakket, enz.) zal het kennis- en ervaringsniveau binnen de doelgroep verschillen. De EDP-auditor zal bij het bepalen van de inhoud en woordkeus van de rapportage uitgaan van een minimumkennis- en ervaringsniveau van de doelgroep. Dit minimumniveau dient aan te sluiten op het deel van de doelgroep met het laagste kennis- en ervaringsniveau.

Door het opnemen van een expliciete opsomming van elk deel van het maatschappelijk verkeer waarvoor een rapport bestemd is, kan elk deel van het maatschappelijk verkeer zelfstandig bepalen of de pakketmededeling voor hem bestemd is. In plaats van een uitputtende opsomming kan ook aangegeven worden voor welk deel respectievelijk welke delen van het maatschappelijk verkeer het rapport niet bestemd is. Een probleem dat hierbij ontstaat is een eenduidige identificatie van de verschillende delen waaruit het maatschappelijk verkeer bestaat. Een mogelijkheid voor identificatie kan zijn het aansluiting zoeken bij de verschillende doelen waarvoor de pakketmededeling naar verwachting van de EDP-auditor gebruikt zal worden. Te denken valt aan de aankoop van een nieuw pakket, de beoordeling van een reeds aangekocht pakket op uitbreidingsmogelijkheden en/of het aansprakelijk stellen van de leverancier wegens wanprestatie.

Het opnemen van een expliciete opsomming van elk deel van het maatschappelijk verkeer waarvoor een rapport bestemd is, is alleen mogelijk indien het identificatieprobleem is opgelost. Immers, anders wordt een bestaande onduidelijkheid vervangen door een nieuwe onduidelijkheid. In dit opzicht is er een rol weggelegd voor alle partijen die betrokken zijn bij de beoordeling van standaardpakketten (opdrachtgevers, gebruikers en EDP-auditors).

**Verstrekker van de uitkomst van de audit**

*Accountantsverklaring*
Wettelijk is bepaald dat uitsluitend de registeraccountant en de accountant met certificerende bevoegdheid bevoegd zijn tot het afgeven van accountantsverklaringen. Iemand kan uitsluitend registeraccountant worden en blijven indien hij voldoet en blijft voldoen aan de kwaliteitseisen die zijn gesteld door de beroepsorganisatie. Deze kwaliteitswaarborgen dienen belanghebbenden voldoende zekerheid te geven dat degene die de accountantsverklaring afgeeft hiervoor voldoende deskundig is.

*Pakketmededeling*
Tot op heden mag eenieder pakketmededelingen afgeven. De opdrachtgever zal uitsluitend de opdracht aan een bepaald individu of bepaalde organisatie verstrekken als hij ervan overtuigd is dat de pakketmededeling voldoende toegevoegde waarde oplevert voor het door hem gestelde doel.

Eerder is reeds aangegeven dat in het geval degene die een pakketmededeling afgeeft Register EDP-auditor is, voor de opdrachtgever en andere belanghebbenden garanties aanwezig zijn omtrent zijn deskundigheid.

## BEWOORDING EN STREKKING VAN HET OORDEEL

Zowel de bewoording als de strekking van het oordeel verdient speciale aandacht.

**Bewoording van het oordeel**

De bewoording dient doelspecifiek te zijn.

*Accountantsverklaring*
Het overgrote deel van het werk van registeraccountants bestaat uit het uitvoeren van controles gericht op de getrouwheid van een financiële verantwoording. In de loop van de jaren is dit werk uitgegroeid tot een geconsolideerde opdracht waarbij gebruikers van de accountantsverklaringen behoefte hebben getoond aan voorgeschreven bewoordingen voor de verklaringen.

Dit heeft geleid tot het opstellen van een voorgeschreven systematiek van oordelen en per oordeel voorgeschreven bewoordingen. Het verklaringenstelsel is dus in een soort keurslijf c.q. confectiepak gegoten. In 1991 heeft het NIVRA het verklaringenstelsel vernieuwd. Dit is gedaan om meer duidelijkheid te verschaffen aan de delen van het maatschappelijk verkeer die gebruikmaken van de accountantsverklaring en om een betere aansluiting te krijgen op de internationale praktijk. Daartoe is een standaardindeling gemaakt met vier mogelijke oordelen, te weten:
- een goedkeurende verklaring;
- een verklaring met beperking;
- een oordeelsonthouding;
- een afkeurende verklaring.

*Pakketmededeling*
Tot heden bestaat er voor pakketmededelingen nog geen voorgeschreven systematiek van oordelen en per oordeel voorgeschreven bewoordingen. Een aantal instanties heeft wel aanbevelingen gedaan, bijvoorbeeld de beroepsorganisatie van de registeraccountants in haar publicatie NIVRA-geschrift 53.

Zolang een algemeen aanvaarde systematiek voor het formuleren van oordelen ontbreekt dienen de voorgeschreven systematiek van oordelen voor de accountantsverklaring en de voorbeeldteksten gezien te worden als het meest geschikte uitgangspunt voor het afgeven van pakketmededelingen. Hierdoor kan optimaal gebruik worden gemaakt van de ervaringen die reeds zijn opgedaan met het verklaringenstelsel en hoeft het wiel niet opnieuw te worden uitgevonden. In de bijlage is voor elke mogelijke strekking van een oordeel, die afzonderlijk is onderscheiden in de voorgaande subparagraaf, een voorbeeldtekst opgenomen. Als basis is gebruikgemaakt van de voorbeeldteksten uit NIVRA-geschrift 53. Deze teksten zijn aangepast om hen geschikt te maken voor pakketmededelingen en ter overbrugging van de in deze paragraaf gesignaleerde verschillen tussen accountantsverklaringen en pakketmededelingen. De teksten zijn voorzover nodig verder aangepast aan de aanbevelingen die tot nu toe in deze subparagrafen naar voren zijn gekomen.

**Strekking van het oordeel**

In deze subparagraaf worden de mogelijke oordelen van accountantsverklaringen vertaald naar pakketmededelingen.

*Goedkeurend oordeel*
Een goedkeurend oordeel houdt in dat de onderzochte kwaliteitsaspecten van het onderzoeksobject naar de mening van de EDP-auditor voldoen aan de gestelde normen.
Indien geen tekortkomingen zijn gesignaleerd die van zodanige ernst zijn dat zij de strekking van het oordeel beïnvloeden en/of onderzoeksonzekerheden zijn gesignaleerd die van zodanige ernst zijn dat zij de strekking van het oordeel beïnvloeden, heeft het oordeel een goedkeurende strekking.

Bij een goedkeurend oordeel kan sprake zijn van tekortkomingen die niet van zodanige ernst zijn dat zij de strekking van het oordeel beïnvloeden. Deze tekortkomingen en aanbevelingen om de tekortkomingen op te heffen dienen niet in het oordeel te worden opgenomen. Zij voegen niets toe aan de strekking van het oordeel. Het verdient de voorkeur om deze in een bijlage van het rapport te

vermelden. Ook kunnen aanbevelingen die buiten de scope van het onderzoek vallen maar tijdens de beoordeling toch als wezenlijk naar voren zijn gekomen, op deze wijze aan de opdrachtgever worden medegedeeld. Gedacht kan worden aan het uitvoeren van bepaalde gebruikerscontroles.

*Oordeel met beperking*
Het oordeel met beperking is een bijzondere verklaring. De EDP-auditor is van mening dat hij een oordeel met een goedkeurende strekking kan geven maar met één of meer beperkingen die ontstaan door onzekerheden met betrekking tot het onderzoek en/of bedenkingen tegen de verantwoording.

Bij een pakketmededeling betekenen geconstateerde onzekerheden met betrekking tot het onderzoek dat de onderzochte kwaliteitsaspecten van het standaardpakket naar de mening van de EDP-auditor voldoen aan de gestelde normen onder voorbehoud van een nader te omschrijven deel van het onderzoeksobject. Als voorbeeld kan worden genoemd een voorbehoud ten aanzien van een kwaliteitsaspect van een bepaalde module.

Bij een pakketmededeling kan niet worden gesproken van het beoordelen van een verantwoording opgesteld door de opdrachtgever, Bij een pakketmededeling dient dan ook gesproken te worden van 'bedenkingen tegen het onderzoeksobject'. Als voorbeeld kan het ontbreken van documentatie worden genoemd van een bepaalde module van het standaardpakket, terwijl de opdrachtgever nadrukkelijk de module als onderdeel ziet van het onderzoeksobject. De EDP-auditor zal dan een voorbehoud moeten maken ten aanzien van deze module.

Het is denkbaar dat een tekortkoming wordt gecompenseerd door een maatregel die buiten het onderzoek valt. Voor de EDP-auditor bestaan de volgende alternatieven:
- de compenserende maatregel onvermeld laten (met handhaving van de beperking);
- nader onderzoek uitvoeren naar de compenserende maatregel en de uitkomst hiervan in het oordeel betrekken (met handhaving van de oorspronkelijke beperking);
- de scope van het onderzoek en de beschrijving van het onderzoeksobject aanpassen. Vervolgens is het oordeel opnieuw te bezien na een aanvullend onderzoek.

Het komt vaak voor dat geconstateerde tekortkomingen al tijdens het onderzoek worden verholpen, of dat acties met dat doel in gang worden gezet. Dit kan worden vermeld in het oordeel, met handhaving van de oorspronkelijke beperkingen.

*Oordeelsonthouding*
Van een oordeelsonthouding is sprake als de EDP-auditor niet tot een totaaloordeel kan komen met betrekking tot normen voor het onderzoeksobject. Hij kan door zijn onderzoek niet vaststellen of het object voor de onderzochte kwaliteitsaspecten voldoet aan de gestelde normen. Een oordeelsonthouding impliceert een combinatie van onderzoekszekerheden van meer materiële betekenis. In accountantsterminologie wordt dit van 'wezenlijke' betekenis genoemd.

In eerste instantie zal de EDP-auditor in overleg met de opdrachtgever kunnen kijken of hij de scope van het onderzoek en de beschrijving van het onderzoeksobject kan aanpassen. Het oordeel dient dan opnieuw te worden bezien na een aanvullend onderzoek. Het aanpassen van de scope van het onderzoek zal niet altijd een oplossing bieden. Als voorbeeld kan worden genoemd dat de productbeschrijving niet aan de eerdergenoemde minimumeisen voldoet, zodat het referentiekader ontbreekt voor de toetsing van de programmatuur zelf.

*Bij een pakketmededeling kan niet worden gesproken van het beoordelen van een verantwoording opgesteld door de opdrachtgever.*

De strekking van de oordeelsonthouding zal bij tekortkomingen snel een negatief karakter krijgen. Daarom verdient het in deze situaties aanbeveling een rapport met bevindingen te verstrekken waarin wordt aangegeven welke onderdelen van het onderzoek voldoen aan de criteria en welke niet.

*Afkeurend oordeel*
Bij een afkeurend oordeel is de EDP-auditor tot de conclusie gekomen dat het onderzoeksobject niet aan de gestelde eisen voldoet. In accountantsterminologie wordt gesproken van een combinatie van tekortkomingen van wezenlijke betekenis.

Een afkeurend oordeel houdt in dat de onderzochte kwaliteitsaspecten van het object van onderzoek naar de mening van de EDP-auditor niet voldoen aan de gestelde normen.
Indien tekortkomingen zijn gesignaleerd die van zodanige ernst zijn dat zij de strekking van het oordeel beïnvloeden en/of onderzoeksonzekerheden zijn gesignaleerd die van zodanige ernst zijn dat zij de strekking van het oordeel beïnvloeden, heeft het oordeel een afkeurende strekking.

## KWANTIFICERING VAN HET PROCES VAN OORDEELSVORMING

In NIVRA-geschrift 53 wordt de mogelijkheid van het vermelden van voorbehouden bij een oordeel uitgesloten, met als belangrijkste motief dat het wegen van voorbehouden een moeilijke zaak is. Dit kan wel zo zijn, maar het kan ook juist als een uitdaging worden gezien. Bovendien dient om tot een goedkeurend of afkeurend oordeel te kunnen komen hetzelfde wegingsproces te worden doorlopen, en speelt dus hetzelfde probleem.

Om te komen tot een oordeel over de getrouwheid van de jaarrekening wordt gebruikgemaakt van het materialiteitsbeginsel. Bij de accountantsverklaring wordt materialiteit veelal gekwantificeerd door de materialiteit in guldens uit te drukken en af te zetten tegen de posten in de jaarrekening. Een materiële tekortkoming/onzekerheid kan worden omschreven als een tekortkoming/onzekerheid die de beslissing van de doelgroep kan beïnvloeden. De accountant neemt globaal gesteld de totale som van alle fouten die hij ontdekt heeft bij de controle van de individuele posten van de jaarrekening en zet deze af tegen het bedrag dat hij van tevoren heeft bepaald als norm voor zijn oordeel (de zogenaamde tolerantie).

Bij een pakketbeoordeling kan helaas geen gebruik worden gemaakt van het in guldens gemeten materialiteitsbeginsel om te komen tot een eindoordeel. De vragen die dan opkomen zijn:
- Welk gewicht kent de EDP-auditor toe aan elke individuele tekortkoming en onzekerheid die in zijn onderzoek naar voren is gekomen om te kunnen komen tot een eindoordeel over de kwaliteit van het onderzoeksobject?
- Hoe is hij gekomen tot de bepaling van deze gewichten?
- Kan de gebruiker zelfstandig vaststellen op welke wijze de EDP-auditor tot zijn eindoordeel is gekomen?

In een voorgaande subparagraaf is reeds aangegeven dat tot heden geen algemeen aanvaarde normen beschikbaar zijn waaraan de kwaliteitsaspecten van een standaardpakket kunnen worden getoetst. Wel worden door verschillende instanties (zoals de grote openbare accountantskantoren en het NIVRA) pogingen ondernomen om bepaalde standaarden op te zetten. Deze ontwikkeling dient als positief te worden ervaren omdat mede hierdoor pakketbeoordeling zich kan ontwikkelen in de richting van een meer geconsolideerde functie.
Juist omdat algemeen aanvaarde normen nog steeds ontbreken lijkt het van groot belang dat de gebruikers van een pakketmededeling inzicht hebben in de door de EDP-auditor gehanteerde normen en de wijze waarop hij tot het oordeel is gekomen. Indien gebruikers dit inzicht niet kunnen verkrijgen, is de basis gelegd voor het ontstaan van een verwachtingskloof tussen de EDP-auditor en degenen die gebruikmaken van de pakketmededeling.

*Het ontstaan van een verwachtingskloof tussen de EDP-auditor en degenen die gebruikmaken van de pakketmededeling, dient te worden voorkomen.*

Om gebruikers dit inzicht te kunnen verschaffen zullen de door de EDP-auditor gehanteerde normen en de wijze waarop hij tot het oordeel is gekomen op een of andere wijze in zijn eindrapportage naar voren moeten komen. Een mogelijkheid om dit te bereiken is het kwantificeren van het oordeelsvormingsproces. Hiervoor kunnen bijvoorbeeld de volgende (additionele) stappen in het beoordelingstraject worden opgenomen:

1. Het eenduidig identificeren van binnen het standaardpakket te onderkennen modules.

2. Het toekennen van een wegingsfactor per kwaliteitsaspect per module. De wegingsfactor bepaalt per module het gewicht van het oordeel over dit aspect in het eindoordeel over dit kwaliteitsaspect op pakketniveau (zie stap 7).
Hierbij gelden de volgende randvoorwaarden:
a. de waarde van deze wegingsfactor dient >= 0 en <= 1 te zijn;
b. de som van deze wegingsfactoren per module dient gelijk te zijn aan 1.

3. Het vaststellen van de normen per kwaliteitsaspect per module. Het kan zijn dat een norm geldt voor meerdere combinaties van kwaliteitsaspecten en modules.

4. Het toekennen van een wegingsfactor uit stap 2 aan elke norm uit stap 3.

5. Het bepalen voor elke norm uit stap 3 of is voldaan aan de norm. Hierbij kan gekozen worden uit de volgende waarden:
a. er is niet voldaan aan de norm: de waarde 0 dient te worden toegekend;
b. er is wel voldaan aan de norm: de waarde 1 dient te worden toegekend.

6. Het berekenen van de score per kwaliteitsaspect *per module* op basis van de uitkomsten van de stappen 2, 4 en 5.
Mogelijkheden: aan de norm voor een kwaliteitsaspect voor een bepaalde module is:
- niet voldaan: de score is gelijk aan de wegingsfactor;
- wel voldaan: de score is gelijk aan 0.

7. Het berekenen van de score per kwaliteitsaspect op *pakketniveau* op basis van de uitkomsten van de stappen 2 en 6.

De opdrachtgever en de EDP-auditor dienen in de fase van opdrachtaanvaarding en -verstrekking overeenstemming te bereiken over de binnen de opdracht te onderscheiden modules, de kwaliteitsaspecten en de inhoud van elk kwaliteitsaspect. Over het algemeen zal hierover weinig verschil van mening bestaan tussen beide partijen; de EDP-auditor kan hierin wel enige concessies doen aan de opdrachtgever mits de gehanteerde definities toereikend worden opgenomen in zowel de opdracht als de eindrapportage.
De EDP-auditor dient echter de stappen 1 tot en met 6 geheel zelfstandig uit te voeren. Afstemming met de opdrachtgever is wel mogelijk, maar de EDP-auditor is uiteindelijk degene die bepaalt op welke wijze hij tot zijn oordeel komt en tot welk oordeel hij komt. De EDP-auditor is tenslotte verantwoordelijk voor de vaktechnische inhoud van de pakketmededeling en niet de opdrachtgever.

De uitkomsten van elke uitgevoerde stap dienen in de eindrapportage van de EDP-auditor te worden

opgenomen zodat potentiële belanghebbenden hiervan kennis kunnen nemen. Gebruikers kunnen mede op basis hiervan voldoende inzicht verkrijgen in de wijze waarop de EDP-auditor tot een goedkeurend oordeel, een oordeel met beperking, een oordeelsonthouding of een afkeurend oordeel is gekomen. Het risico op het ontstaan van een verwachtingskloof tussen de EDP-auditor en degenen die gebruikmaken van de pakketmededeling wordt hierdoor aanzienlijk beperkt.

## OVERIGE AANDACHTSPUNTEN

In deze paragraaf wordt nog een aantal aandachtspunten behandeld die van belang zijn voor de betekenis die de doelgroep mag ontlenen aan een pakketmededeling.

### Geldigheidsperiode

In de pakketmededeling dient in verband met de afbakening van de verantwoordelijkheid van de EDP-auditor, de datum waarop of de periode waarin de beoordeling is uitgevoerd, te worden opgenomen. De begrenzing van de verantwoordelijkheid van de EDP-auditor voor de toekomst wordt nog eens expliciet tot uitdrukking gebracht doordat hij de mededeling dateert. Tussen de datum of de periode waarop de pakketmededeling betrekking heeft en het moment van afgifte van de pakketmededeling zal normaliter enige tijd liggen. Indien in deze tussenliggende periode ten aanzien van het object van onderzoek zich zodanige omstandigheden voordoen dat de strekking van het oordeel wordt aangetast, dan is het de taak van de EDP-auditor hiervan in zijn oordeel melding te maken.

### Ondertekening

Met het vermelden van de plaats van afgifte van het oordeel wordt bij eventuele juridische aangelegenheden domicilie gekozen. Daarnaast wordt duidelijk gemaakt waar inlichtingen kunnen worden ingewonnen. Door ondertekening van de mededeling wordt de mededeling gewaarmerkt. De auditor kan de mededeling waarmerken met zijn eigen naam en/of met de firmanaam.

### Samenhang oordeel en rapportage

Een oordeel over de kwaliteit van een standaardpakket kan alleen op zijn strekking worden beoordeeld in samenhang met de in de rapportage opgenomen bijlagen. De EDP-auditor dient in het rapport op te nemen dat het oordeel uitsluitend met de gehele rapportage mag worden verstrekt. In de rapportage dient te worden opgenomen dat de verstrekking alleen mag plaatsvinden aan de in de rapportage beschreven delen van het maatschappelijk verkeer die behoren tot de doelgroep. Indien de opdrachtgever de rapportage aan anderen wil verstrekken, dient hij hiervoor expliciet toestemming te vragen aan de EDP-auditor.

Indien de opdrachtgever de pakketmededeling voor commerciële doeleinden wil aanwenden, zal hij zijn potentiële kopers attent willen maken op de door de auditor afgegeven pakketmededeling. Voor een effectieve communicatie met potentiële kopers zal de opdrachtgever een korte en krachtige opmerking willen opnemen in de advertentie of een andere commerciële uiting. Het is aan te bevelen in de rapportage op te nemen onder welke voorwaarden en met welke tekst de opdrachtgever een verwijzing naar de pakketmededeling mag opnemen in zijn commerciële uiting. De EDP-auditor dient te voorkomen dat de opdrachtgever een zogenaamde 'zwijgende verwijzing' opneemt, hetgeen betekent dat de opdrachtgever vermeldt dat een pakketmededeling is afgegeven zonder aan te geven wat de strekking is van het oordeel. Deze zaken dienen tevens in de opdrachtverstrekking te worden vastgelegd.

## VOORSTEL TOT STANDAARDISATIE

Het scala van werkzaamheden dat door de EDP-auditor wordt uitgevoerd en van de objecten die de EDP-auditor controleert, is zo breed dat de uitingen van de EDP-auditor niet in eenzelfde keurslijf als van het verklaringenstelsel van de accountant gegoten kunnen worden. Wel is het mogelijk om per soort EDP-audit een bepaalde mate van standaardisatie door te voeren in vorm, formulering en inhoud van de rapportage van de EDP-auditor over de uitkomsten van de door hem uitgevoerde audit. Hierbij is een rol weggelegd voor alle partijen die betrokken zijn bij de beoordeling van standaardpakketten.

In tabel 4 is een voorstel opgenomen voor de standaardisatie van een pakketmededeling afgegeven door een EDP-auditor waarin alle aanbevelingen die in dit artikel naar voren zijn gekomen, zijn verwerkt. Om de pakketmededeling leesbaar te houden is het aan te bevelen om een aantal van deze gegevens in de bijlage van de pakketmededeling op te nemen. Tabel 5 bevat een opsomming van deze gegevens.
Dit voorstel kan door alle partijen die betrokken zijn bij de beoordeling van standaardpakketten worden gebruikt bij het opstellen en het hanteren van een pakketmededeling.

## CONCLUSIES

Aan het eind van het beoordelingsproces zal de EDP-auditor zich een oordeel dienen te vormen over de mate waarin het standaardpakket voor elk kwaliteitsaspect voldoet aan de gestelde normen en de uitkomsten van zijn beoordeling kenbaar moeten maken aan de doelgroep waarvoor deze uitkomsten bestemd zijn. Dit zijn de opdrachtgever en eventuele andere belanghebbenden. Veelal zal dit op een schriftelijke wijze gebeuren. De vorm, de formulering en de inhoud van het oordeel wekken verwachtingen bij deze doelgroep. Een pakketmededeling vormt de schriftelijke rapportage van een

**In de pakketmededeling op te nemen punten**

- De identificatie van de opdrachtgever (naam, adres);
- de identificatie van de uitvoerder;
- een verwijzing naar de verleende opdracht en/of de opdrachtformulering zelf;
- de periode waarin het onderzoek heeft plaatsgevonden.

- Het object:
  - de identificatie van het object: naam, versie- en releasenummer en datum;
  - een opsomming van de onderzochte modules.

- De onderzochte kwaliteitsaspecten:
  - een opsomming van de onderzochte kwaliteitsaspecten in relatie tot het object;
  - een omschrijving van elk onderzocht kwaliteitsaspect in relatie tot het object.

- Het oordeel van de auditor:
  - de strekking van het oordeel;
  - het oordeel is gebaseerd op de door de auditor verrichte werkzaamheden;
  - een oordeel per onderzocht kwaliteitsaspect;
  - een omschrijving van eventuele voorbehouden die worden gemaakt bij het gevormde oordeel per onderzocht kwaliteitsaspect indien hun gezamenlijk belang het oordeel van de auditor heeft beïnvloed;
  - de diepgang van het onderzoek: de opzet of de opzet en het bestaan.

- De beperkingen of afbakeningen van punten die niet zijn onderzocht, zoals:
  - de toetsing van de overeenkomst van beoordeelde documentatie en de software;
  - indien van toepassing een opsomming van de niet-onderzochte modules;
  - de kwaliteit van de procedures en de maatregelen die in de gebruikers- en automatiseringsorganisatie zijn getroffen;
  - de wijzigingen in de programmatuur die zijn aangebracht na de datum van de mededeling;
  - de wijzigingen in de documentatie die zijn aangebracht na de datum van de mededeling;
  - het feit dat de werking van de in het object opgenomen internecontrolemaatregelen niet is onderzocht;
  - het feit dat het oordeel uitsluitend geldt voor het gebruikte platform;
  - een omschrijving van het gebruikte computerplatform (besturingssysteem, omvang interne geheugen, aantal terminals en printers, etc., afhankelijk van de beoordeelde kwaliteitsaspecten);
  - eventueel aanwezige mogelijkheden om via systeemutilities gegevens te veranderen.

- Verstrekking van het rapport aan de doelgroep:
  - het feit dat het rapport slechts in zijn geheel aan derden ter inzage mag worden verstrekt;
  - vermelding aan wie het rapport verstrekt mag worden;
  - het feit of een verwijzing mag worden opgenomen naar de mededeling en/of het rapport;
  - de tekst die moet worden gebruikt indien deze verwijzing plaatsvindt.

- Ondertekening door de auditor:
  - de naam van het bedrijf of individuele personen;
  - de plaats en de datum (dag, maand, jaar) van ondertekening.

*Tabel 4. Op te nemen punten in een pakketmededeling.*

beoordeling op één of meer kwaliteitsaspecten van standaardpakketten.
De schriftelijke rapportage dient op een zodanige wijze te worden samengesteld dat de kans op interpretatieverschillen tussen de gebruikers van de mededeling en degene die de mededeling heeft afgegeven zo beperkt mogelijk wordt gehouden.

Om het ontstaan van een verwachtingskloof door interpretatieverschillen inzake de betekenis van een pakketmededeling te beperken is het van belang dat de in dit artikel genoemde aanbevelingen

**In de bijlage bij de pakketmededeling op te nemen punten**

- Een overzicht van de functionaliteiten die zijn beoordeeld;
- een uitgebreide beschrijving van de gehanteerde normen ingedeeld naar module en/of per kwaliteitsaspect;
- een omschrijving van de functionaliteiten van het pakket;
- een omschrijving van de gebruikte documentatie: soort, helpfunctie, versienummer, datum;
- een omschrijving van de gebruikte output (omschrijving, functienaam);
- een omschrijving van de gebruikte testset;
- een beschrijving van de uitgevoerde stappen zoals is beschreven in de paragraaf over het kwantificeren van het oordeelsvormingsproces;
- een beschrijving van de uitkomsten van de uitgevoerde stappen zoals is beschreven in de paragraaf over het kwantificeren van het oordeelsvormingsproces;
- een omschrijving van eventuele voorbehouden die worden gemaakt bij het gevormde oordeel per onderzocht kwaliteitsaspect indien hun gezamenlijk belang het oordeel van de auditor niet beïnvloedt of het oordeel niet anders zou zijn indien de voorbehouden niet aanwezig zouden zijn;
- een opsomming van in het onderzoek naar voren gekomen attentiepunten voor de pakketgebruikers (bevindingen en aanbevelingen);
- een opsomming en een omschrijving van de attentiepunten voor de leverancier (norm, bevinding en aanbeveling ter verbetering van pakket).

*Tabel 5. Punten voor de bijlage bij een pakketmededeling.*

in de rapportage worden opgenomen. In ieder geval dienen het object, de beoordeelde kwaliteitsaspecten in relatie tot het object, de per kwaliteitsaspect gehanteerde normen en het oordeel per kwaliteitsaspect aan de doelgroep te worden medegedeeld. Het is aan te bevelen de doelgroep inzicht te geven in de wijze waarop de EDP-auditor tot zijn oordeel is gekomen zolang een algemeen aanvaarde set van normen ontbreekt. Hierdoor krijgt elk deel van het maatschappelijk verkeer een adequate mogelijkheid om zelfstandig vast te stellen:

- of zij zekerheid *mogen* ontlenen aan de pakketmededeling door vaststelling of zij behoren tot de doelgroep waarvoor de pakketmededeling bestemd is en waarop zij qua formulering, vorm en inhoud is afgestemd, en
- in welke mate zij zekerheid *kunnen* ontlenen aan de pakketmededeling door kennisneming van de per kwaliteitsaspect gehanteerde normen, het gevormde oordeel en de wijze waarop de EDP-auditor tot dit oordeel is gekomen.

## LITERATUUR


[Goos84] B. Goossens RA, *Certificering van Software en EDP-auditing*, NGI Symposium: Certificering van software, november 1984.

[Init86] Initiatiefgroep software certificering, *Naar geprogrammeerde kwaliteit: Keuring en certificering van programmapakketten*, november 1986.

[Kamp82] Drs. H.A. Kampert, *Mededelingen met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking – een kloof tussen rationele behoeften en het vermogen van de accountant?*, De Accountant nr. 4, december 1982, p. 234-240.

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

[Keur86] *Naar geprogrammeerde kwaliteit, Keuring en certificatie van programmapakketten*, november 1986.

[Limp33] Th. Limperg jr., *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.

[Neis87] A.W. Neisingh RE RA, *Keuring en certificering van informatietechnologieproducten*, EDP-audit volwassen?, SIC-NGI, 1987.

[Neis89] A.W. Neisingh RE RA, *Keuring en certificering van informatietechnologieproducten*, NGI-seminar, 1989, blz. 1-8.

[Niel84] Prof. dr. ir. G.C. Nielen, *Certificering van software: noodzakelijk of zinloos?*, NGI-Symposium: Certificering van software, november 1984, blz. 11-20.

[NIVR] NIVRA, *1.01 Algemeen kader met betrekking tot controle en daaraan verwante opdrachten; 5.04 Onzekerheden en bedenkingen; 5.03 De accountantsverklaring*; Richtlijnen Controle.

[NIVR82] NIVRA-geschrift 26, *Automatisering en controle*, Kluwer Deventer, februari 1982.

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

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

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

[NIVR95a] NIVRA-studierapport 19, *Accountant en ISO 9000-certificering*, september 1995.

[NIVR95b] NIVRA, *Nieuwe teksten voor beoordelings- en samenstellingsopdrachten*, NIVRA-berichten, 29e jaargang, no. 2, oktober 1995.

[Praa93] J. van Praat, *De NOREA en de RAAD voor Certificatie?*, de EDP-Auditor, nr. 1, januari 1993, blz. 28-33.

[Prog85] *Programmeerkwaliteit, Objectieve leveranciersbeoordeling en de kwaliteit van programmatuur*, juni 1985.

[Roos87] H. Roos RA, *Mededelingen over de uitkomst van EDP-audits; grondslag, strekking en vorm*, EDP-audit volwassen?, SIC-NGI, 1987, blz. 29-52.

[Sijbr96] Drs. H.E. Sijbring RE RA, *De EDP-auditor: vertrouwensman, agent of ...?*, Compact 1996/3.

[Stra85] A. Straatman RA, *Accountantsoordelen inzake applicatiesoftware*, Maandblad voor Accountancy en Bedrijfshuishoudkunde, 1985, 10/11, blz. 441-447.

[Urba86] J.H. Urbanus, *De invloed van software-certificering op de ontwikkeling van de EDP-audit als een bijzondere opdracht*, in: 24 Over EDP-auditing, 1986, blz. 26-32.

[Velt96] Drs. P. Veltman RE RA, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 1995/3.

[Ngis88] Werkgroep EDP-audit Standaarden, *Studierapport EDP-audit Standaarden*, SIC-NGI 1988.

[Zwar92] H. de Zwart RA, *Rapportering door EDP-auditors*, in: Handboek voor EDP-auditing, afl. 5, december 1992, blz. C. 4.4-01-31.



*Drs. H. E. Sijbring RE RA*
*Is van 1991 tot september 1994 werkzaam geweest in de controlepraktijk van KPMG. Sinds september 1994 is hij werkzaam bij KPMG EDP Auditors, op dit moment als EDP-auditmanager. Hij richt zich voornamelijk op het uitvoeren van onderzoeken gericht op het beoordelen en adviseren op het gebied van gebruikersorganisatie en systeemontwikkeling.*
*Hij heeft zich daarnaast gespecialiseerd in interne controle in en rondom geïntegreerde standaardsoftwarepakketten. De nadruk ligt hierbij op het pakket SAP. Hij is op dat gebied betrokken bij het geven van cursussen.*

# BIJLAGE: VOORBEELDEN VAN BEWOORDINGEN VOOR OORDELEN IN EEN PAKKETMEDEDELING

### a. Goedkeurend oordeel

Hieronder volgt de formulering voor een mededeling met een goedkeurende strekking. Hierbij is uitsluitend het oordeel weergegeven en niet het gehele onderzoeksrapport. Elk kwaliteitsaspect dient in het oordeel duidelijk te worden omschreven.

Aan: ..... [opdrachtgever]

[Aanhef]

In uw opdracht hebben wij een onderzoek ingesteld naar ..... [kwaliteitsaspect] van ..... [object] ten behoeve van ..... [doelgroep]. Onder ..... [aspect] is in ons onderzoek verstaan ..... [definitie aspect].
Onder ..... [object] is in dit onderzoek verstaan .... [omschrijving, datering etc.].

Op grond van onderzoek zijn wij van oordeel dat ..... [object] in *voldoende* mate beantwoordt aan de eisen van .... [norm].

Hierna treft u een gedetailleerde weergave van onze bevindingen.

.... [plaats], ..... [dagtekening]
.... [ondertekening]

### b. Goedkeurend oordeel met beperking

Hieronder volgt de formulering voor een mededeling met een goedkeurende strekking maar met een aantal beperkingen. Hierbij is alleen het gedeelte weergegeven dat afwijkt van de voorgestelde formulering voor een mededeling met een goedkeurend oordeel zonder beperkingen. Elk kwaliteitsaspect waarvoor een beperking geldt dient in het oordeel expliciet te worden vermeld.

Op grond van onderzoek zijn wij van oordeel dat ..... [object] in *voldoende* mate beantwoordt aan de eisen van .... [norm] *met uitzondering van* ..... [kwaliteitsaspect] van ..... [deel van het object/object zelf].

Hierna treft u een gedetailleerde weergave van onze bevindingen.

### c. Oordeelsonthouding

Hieronder volgt de formulering voor een mededeling met een oordeelsonthouding. Hierbij is alleen het gedeelte weergegeven dat afwijkt van de voorgestelde formulering voor een mededeling met een goedkeurend oordeel.

Wij hebben .....[omschrijving tekortkoming] geconstateerd die echter gezien ..... [beperking] niet op korte termijn kan worden opgeheven.

Op grond van deze tekortkoming *onthouden* wij ons van een *oordeel* over ..... [object] als *geheel*.
Wel zijn wij op grond van het onderzoek van oordeel dat overigens toereikende maatregelen ter voldoening aan de eisen van ..... [aspect] zijn getroffen.

### d. Afkeurend oordeel

Hieronder volgt de formulering voor een pakketmededeling met een afkeurend oordeel. Hierbij is alleen het gedeelte weergegeven dat afwijkt van de voorgestelde formulering voor een mededeling met een goedkeurend oordeel.

Wij hebben vastgesteld dat .....[tekortkoming].
Op grond van onderzoek zijn wij van oordeel dat ..... [object] in onvoldoende mate beantwoordt aan de eisen van ..... [aspect].

# Voorschrift Informatiebeveiliging Rijksdienst

Mw. drs. M.C.C. van der Burg RI en
J.M.W. van de Garde RE

**Op grond van het Voorschrift Informatiebeveiliging Rijksdienst 1994 moet voor alle informatiesystemen en verantwoordelijkheidsgebieden binnen de Rijksdienst zijn bepaald welk stelsel van maatregelen uit hoofde van de informatiebeveiliging getroffen dient te zijn. Een mogelijke uitwerking van de op grond van het voorschrift uit te voeren afhankelijkheids- en kwetsbaarheidsanalyse is in dit artikel weergegeven.**

## INLEIDING

Sinds 1 januari 1995 is het Voorschrift Informatiebeveiliging Rijksdienst 1994 (VIR94) van kracht. Op grond van dit voorschrift moet voor alle informatiesystemen en verantwoordelijkheidsgebieden binnen de Rijksdienst zijn bepaald welk stelsel van maatregelen uit hoofde van de informatiebeveiliging getroffen dient te zijn. Het voorschrift duidt aan dat dit stelsel van maatregelen moet worden vastgesteld door het uitvoeren van een afhankelijkheids- en kwetsbaarheidsanalyse. Dit is echter niet verder uitgewerkt. Zowel het opstellen van een beveiligingsplan als de implementatie van de noodzakelijke maatregelen zou per 1 januari 1997 moeten zijn gerealiseerd. De stand van zaken over de invoering van VIR94 is gerapporteerd aan de Minister van Binnenlandse Zaken. De onduidelijkheid over de wijze van opstellen van een informatiebeveiligingsplan heeft bij veel departementen geleid tot vertraging in de uitvoering van deze werkzaamheden. Uitstel zal echter niet mogen leiden tot afstel. Een mogelijke uitwerking van de afhankelijkheids- en kwetsbaarheidsanalyse is in dit artikel weergegeven.

## GESCHIEDENIS

In 1988 is door de Algemene Rekenkamer het rapport Computerbeveiliging[1] uitgebracht. In dit rapport constateert de Rekenkamer dat het afdekken van risico's wat betreft gegevens in geautomatiseerde systemen bij de ministeries in onvoldoende mate wordt gewaarborgd.
Door technologische ontwikkelingen[2] op het gebied van informatievoorziening en door een veranderend inzicht in de wijze waarop de diverse overheidsorganisaties moeten worden aangestuurd en beheerd[3], worden geautomatiseerde informatiesystemen echter ook voor overheidsorganen steeds belangrijker voor de bestuurs- en bedrijfsprocessen.

Bovenstaande ontwikkelingen zijn er mede de oorzaak van dat de bestaande regelgeving op het gebied van informatiebeveiliging niet meer voldoende aansluit bij de huidige stand van zaken dan wel te specifiek is gericht op een bepaald soort gegeven.[4] Het kabinet besluit dan ook dat een begin moet worden gemaakt met de aanpassing en vernieuwing van de regelgeving.
Dit kabinetsbesluit heeft uiteindelijk geresulteerd in het besluit Voorschrift Informatiebeveiliging Rijksdienst 1994 (VIR94). In het voorschrift is, zoals in de algemene toelichting op dit voorschrift is vermeld, in 'hoofdlijnen' vastgelegd waaraan het informatiebeveiligingsbeleid moet voldoen. In het voorschrift zijn de formele regels vastgelegd waaraan elk ministerie zich moet houden. Het voorschrift moet als zodanig 'steun en houvast' bieden bij het te voeren informatiebeveiligingsbeleid.[5]

Het beveiligingsbeleid dient uiteindelijk een informatiebeveiligingsplan per verantwoordelijkheidsgebied[6] en/of informatiesysteem op te leveren. Met een kwetsbaarheidsanalyse moet kunnen worden aangetoond dat, met de in het plan opgenomen maatregelen, aan de gestelde betrouwbaarheidseisen kan worden voldaan. Deze betrouwbaarheidseisen op hun beurt moeten worden bepaald door het uitvoeren van een afhankelijkheidsanalyse. In het voorschrift wordt niet aangegeven op welke wijze beide analyses uitgevoerd kunnen/moeten worden. De uitvoering wordt overgelaten aan de afzonderlijke departementen.
Binnen een departement is de beveiliging van de informatiesystemen/verantwoordelijkheidsgebieden de taak van het lijnmanagement. De deskundigheid van de lijnmanagers zal doorgaans niet op het terrein van de beveiliging liggen. Een nadere uitwerking van de begrippen afhankelijkheidsanalyse en kwetsbaarheidsanalyse zal een handreiking naar deze functionarissen zijn en ertoe kunnen leiden dat het opstellen van een beveiligingsplan op een eenduidige wijze zal gebeuren.
Daar de geautomatiseerde informatievoorziening niet meer voornamelijk plaatsvindt in gespecialiseerde organisatie-eenheden, maar op alle werkplekken van overheidsorganisaties, is de informatievoorzieningsfunctie gediversifieerder dan voorheen. Hierdoor zal elk departement afzonderlijke eisen stellen aan de informatiebeveiliging.

## VOORSCHRIFT INFORMATIEBEVEILIGING RIJKSDIENST 1994

De belangrijke plaats van de informatievoorziening in de bedrijfs- en bestuursprocessen binnen de overheid vereist regelgeving voor beveiliging. Hoewel de beveiliging van de informatie en de informatievoorzieningsprocessen de verantwoordelijkheid is van de afzonderlijke ministeries, is een overheidsbrede regelgeving toch van belang. De informatievoorzieningsprocessen van één ministerie hebben doorgaans niet alleen invloed op het functioneren van de desbetreffende organisatie maar ook op het functioneren van derden (andere departementen, lagere overheden, bedrijven, burgers). De snel voortschrijdende ontwikkeling op onder andere technologisch en organisatorisch gebied maakt een zekere flexibiliteit zeer wenselijk. Het voorschrijven van technische maatregelen is niet zinvol, ze zouden immers op korte termijn zijn achterhaald. In het Voorschrift Informatiebeveiliging Rijksdienst 1994 is daarom gekozen voor het beschrijven van de stappen waarmee 'tot een evenwichtig pakket van maatregelen voor de informatiebeveiliging' wordt gekomen. De stappen moeten uiteindelijk resulteren in een informatiebeveiligingsplan.

In 1994 wordt een interdepartementaal overlegorgaan, het IB-beraad, ingesteld. Het IB-beraad is een overleg tussen de plaatsvervangend Secretarissen-Generaal (PSG's) van de diverse departementen. In het IB-beraad vindt overleg plaats over diverse facetten van de (inter-)departementale informatiebeveiliging.

### Doelgroep

VIR94 is van toepassing op de Rijksdienst. Hiertoe behoren alle ministeries met de daaronder ressorterende diensten, bedrijven en instellingen. Er is een discussie gaande of VIR94 ook van toepassing moet worden verklaard voor de Zelfstandige Bestuurs Organen.

De secretaris-generaal van elk ministerie moet een beleidsdocument voor informatiebeveiliging voor het gehele ministerie opstellen en uitdragen. Daarnaast is in dit voorschrift vastgelegd dat de lijnmanagers die de verantwoordelijkheid hebben voor een informatiesysteem, inhoud moeten geven aan de informatiebeveiliging van het systeem.

### Inhoud

VIR94 geeft op hoofdlijnen aan waaraan het informatiebeveiligingsbeleid moet voldoen. Gedetailleerde richtlijnen voor het opstellen van een beveiligingsplan ontbreken dus.
Het voorschrift bestaat uit een zestal artikelen. In deze zes artikelen is de organisatie en de aanpak van de informatiebeveiliging bij de rijksoverheid uitgewerkt. Het VIR94 beschrijft in hoofdlijnen waar de verantwoordelijkheden voor de informatiebeveiliging liggen, welke vorm en inhoud het beveiligingsbeleid moet hebben en hoe de gewens-

te mate van beveiliging moet worden vastgesteld en gehandhaafd.
In dit artikel zullen de begrippen afhankelijkheidsanalyse en kwetsbaarheidsanalyse nader worden uitgewerkt.

## RISICOANALYSE

Het doel van (informatie)beveiligingsmaatregelen is het tegengaan van mogelijke kwalijke gevolgen voor het bedrijfs- of bestuursproces veroorzaakt doordat dreigingen de betrouwbaarheid van de informatievoorziening ondermijnen. Beveiliging van de informatievoorziening brengt echter kosten met zich mee. Er zal bij de implementatie van beveiligingsmaatregelen daarom een gedegen kosten-batenanalyse moeten plaatsvinden. Als immers de kosten van de beveiliging hoger zijn dan de waarde van de te beveiligen informatie, moet men zich afvragen of men het doel niet voorbij is geschoten en moet men misschien zelfs overwegen of de registratie van die gegevens nog wel zinvol of noodzakelijk is. VIR94 spreekt van een 'evenwichtig' pakket van maatregelen[7] die de betrouwbaarheidseisen, gegeven de in beschouwing genomen bedreigingen, realiseren.

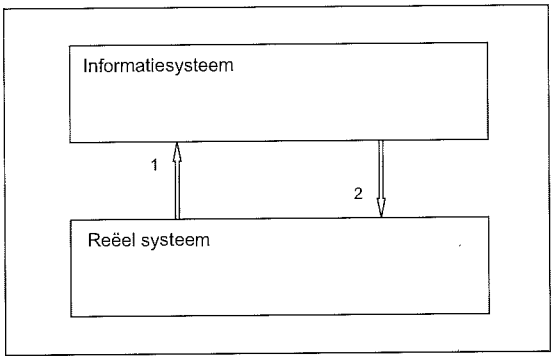
Wil men op verantwoorde wijze een beveiligingsplan opstellen dan moet men ten minste weten tegen welke risico's men wil beveiligen. Een methode die kan worden gebruikt voor het bepalen van de benodigde beveiligingsmaatregelen is de risicoanalyse.[8]

In VIR94 is bewust gekozen voor het niet gebruiken van het begrip risicoanalyse maar van de begrippen afhankelijkheids- en kwetsbaarheidsanalyse. Bij risicoanalyse wordt het risico uitgedrukt in een kwantitatieve waarde (kans x schade). Bij de overheid is het risico echter doorgaans niet uit te drukken in een kwantitatieve waarde maar is vooral het kwalitatieve aspect van belang. De schade kan bijvoorbeeld worden uitgedrukt in kamervragen aan de minister van een departement (schade aan het imago), ongewenste publiciteit, onvrede bij burgers, het in gevaar brengen van de landsbelangen, etc.
De onderverdeling in afhankelijkheids- en kwetsbaarheidsanalyse (A- en K-analyse) is nodig daar voor het uitvoeren van beide analyses een andere deskundigheid nodig is. Bij de afhankelijkheidsanalyse is een grondige kennis van de bestuurs- of bedrijfsprocessen noodzakelijk. Deze deskundigheid is aanwezig bij de lijnmanager verantwoordelijk voor het desbetreffende proces. De kwetsbaarheidsanalyse vereist veel kennis van informatiebeveiliging en is dus het werkgebied van beveiligingsspecialisten.
De stappen die noodzakelijk zijn bij het uitvoeren van een A- en K-analyse zijn schematisch weergegeven in figuur 2.

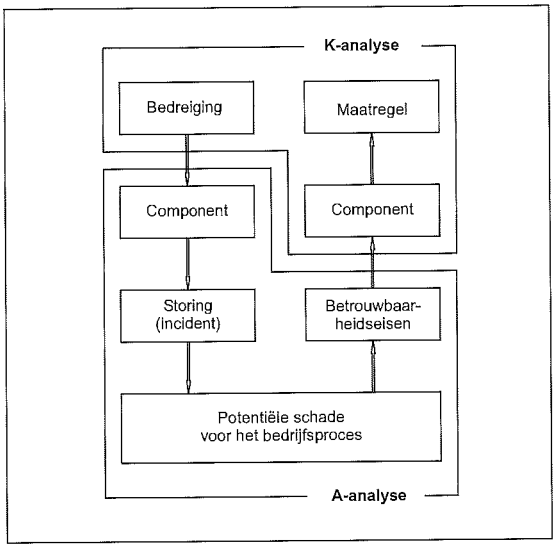
## AFHANKELIJKHEIDSANALYSE

Met behulp van de afhankelijkheidsanalyse[9] wordt vastgesteld wat de gevolgen zijn voor het bedrijfsproces als de betrouwbaarheid van de informatievoorziening te wensen overlaat. Dus, wat is de schade voor het bedrijfsproces als de gegevens die zijn vastgelegd in een ondersteunend informatiesysteem niet voldoen aan de kwaliteitscriteria beschikbaarheid, integriteit en exclusiviteit. De mogelijke schade voor het bedrijfsproces door storingen in de informatievoorziening kan worden onderscheiden in directe, herstel- en/of gevolgschade.[10] De gevolgen van storingen in de informatievoorziening voor het bedrijfsproces kunnen alleen op een adequate wijze worden bepaald door personen die een goed inzicht hebben in het desbetreffende bedrijfsproces. In VIR94 is de lijnmanager daarom verantwoordelijk gesteld voor het opstellen van een beveiligingsplan.[11]
Bestuurs- en bedrijfsprocessen zijn in (bijna) alle gevallen afhankelijk van één of meer informatiesystemen. De relatie tussen bestuurs- en bedrijfsprocessen en een informatiesysteem kan worden weergegeven met het afbeeldingsparadigma[12] (figuur 1).

In dit afbeeldingsparadigma is een tweetal stromen te onderkennen, te weten:
1. gegevens over de werkelijkheid[13];
2. beïnvloeding van het gedrag in de werkelijkheid.[14]




*Figuur 1. Afbeeldingsparadigma.*




*Figuur 2. Stappenplan A/K-analyse.*

Bij het uitvoeren van een afhankelijkheidsanalyse worden, nadat is vastgesteld welke potentiële schaden zich kunnen voordoen bij verstoringen in de informatievoorziening, de betrouwbaarheidseisen gesteld. Hierbij wordt de volgende weg bewandeld. Het uitgangspunt is een bedreiging.[15] Bij het manifest worden van een bedreiging heeft dit gevolgen voor de beschikbaarheid of de goede werking van een IT-component. Zodra de beschikbaarheid of de goede werking van de IT-component niet meer is gewaarborgd, zal dit een storing in de informatievoorziening (incident) veroorzaken. Aan de kwaliteitseisen die worden gesteld aan de informatievoorzieningen kan op dat moment niet meer worden voldaan. Door het niet voldoen aan de kwaliteitscriteria van de informatievoorziening kunnen potentiële schaden optreden bij de door de informatievoorziening ondersteunde bedrijfs- of bestuursprocessen. De mogelijke schaden voor de bestuurs- en bedrijfsprocessen bepalen de betrouwbaarheidseisen die worden gesteld aan het informatiesysteem en dus aan de componenten waaruit dit systeem is opgebouwd. De mogelijke schaden kunnen worden gerangschikt naar oplopende ernst. Dat wil zeggen dat men per onderkende schade een aantal scenario's kan onderscheiden.[16]
Het niet voldoen aan de kwaliteitscriteria van het informatiesysteem of verantwoordelijkheidsgebied kan per bedrijfsproces andere gevolgen hebben.[17]
De potentiële schade en de ernst hiervan zijn afhankelijk van het soort bedrijfsproces. Bij het vaststellen van de betrouwbaarheidseisen zal gezocht moeten worden naar het kleinste gemeenschappelijke veelvoud van de onderkende schaden. De potentiële schaden voor een bedrijfsproces als gevolg van storingen in het informatiesysteem of verantwoordelijkheidsgebied kunnen legio zijn.

Samengevat zijn de stappen die doorlopen moeten worden bij een afhankelijkheidsanalyse:

*Stap 1 – Aangeven wat de relatie is tussen bedrijfs- en bestuursprocessen en informatiesystemen*
Deze stap is nodig voor het verkrijgen van inzicht in het belang van de beschouwde processen voor de organisatie en voor het verkrijgen van inzicht in het belang van het informatiesysteem in (de diverse fasen van) het bedrijfsproces.

*Stap A2 – Vastleggen van de relatie tussen mogelijke storingen in de informatievoorziening en de mogelijke schade voor het bestuurs- of bedrijfsproces*
Het verband tussen een storing in de informatievoorziening en de gevolgen (schade) hiervan voor het bedrijfsproces (potentiële schaden) moet worden vastgelegd. Dit bepaalt de betrouwbaarheidseisen voor de informatievoorziening. De eisen die aan de informatievoorziening worden gesteld, zijn immers een spiegel van de verwachte schade. Een lijnmanager is doorgaans goed in staat aan te geven wat de gevolgen zijn voor het bedrijfsproces als de benodigde informatie niet voldoet aan de noodzakelijke kwaliteitseisen.

*Stap A3 – Inventarisatie IT-componenten*
Als bekend is welke potentiële schaden voor de betrokken bedrijfs- en bestuursprocessen worden veroorzaakt door storingen in de informatievoorziening, moet een beeld worden verkregen van de bedreigingen[18] die de relevante storingen in het informatiesysteem veroorzaken. Een storing in een informatiesysteem wordt veroorzaakt door het niet of niet juist werken van één of meer elementen waaruit een informatiesysteem is samengesteld. Daarom is het van belang alle relevante componenten, zoals gegevens, programmatuur, hardware of infrastructuur, te kennen. Deze worden in deze stap geïnventariseerd.

*Stap A4 – Formuleren betrouwbaarheidseisen per IT-component*
Nadat inventarisatie van de onderkende componenten heeft plaatsgevonden, worden aan alle componenten betrouwbaarheidseisen toegekend. Deze koppeling is noodzakelijk om te kunnen komen tot een evenwichtig pakket beveiligingsmaatregelen. Dit houdt in dat de beveiliging in overeenstemming moet zijn met de waarde van de te beveiligen componenten. Voor de componenten gegevens en programmatuur worden de betrouwbaarheidseisen geformuleerd voortkomend uit de potentiële schade voor het bedrijfsproces door het manifest worden van een bedreiging. Fysieke componenten hebben een geldelijke waarde (vervangingswaarde/waarde instandhouding). De fysieke componenten staan echter niet los van de overige IT-componenten. Bij het formuleren van de betrouwbaarheidseisen moet met beide aspecten rekening worden gehouden. Een adequate beveiliging van deze IT-voorzieningen is daarom niet alleen afhankelijk van de vervangingswaarde van de component. De betrouwbaarheidseisen van deze fysieke componenten worden mede bepaald door de gegevens en de applicatie die deze IT-voorziening als platform hebben en die daarom afhankelijk zijn van deze fysieke componenten. In tabel 1 is samengevat op welke wijze de betrouwbaarheidseisen van de fysieke componenten worden bepaald.

*Stap A5 – Kwantificeren betrouwbaarheidseisen*
Na het uitvoeren van de vorige stappen heeft men inzicht in de kwalitatieve betrouwbaarheidseisen die relevant zijn voor het te onderzoeken informatiesysteem of verantwoordelijkheidsgebied. De formulering van de betrouwbaarheidseisen is gebaseerd op mogelijke schade voor de bedrijfs- of

*Tabel 1. Betrouwbaarheid fysieke componenten.*

| | *Betrouwbaarheidseisen gegevens > betrouwbaarheidseisen IT-voorziening* | *Betrouwbaarheidseisen gegevens < = betrouwbaarheidseisen IT-voorziening* |
|---|---|---|
| Gegevens | eisen gegevens/programmatuur | eisen gegevens/programmatuur |
| IT-voorziening | eisen gegevens/programmatuur | eisen IT-voorziening |

bestuursprocessen. Voor het verkrijgen van een beter inzicht in de betrouwbaarheidseisen is het zinvol de kwalitatieve waardering te kwantificeren.
Het vertalen van de schade in een kwantitatieve waarde is, voorzover dit geen geldbedragen zijn, doorgaans een stuk moeilijker en erg afhankelijk van de individuele beleving van de betrokken manager. Mogelijke schaden moeten daarom op een centraal niveau binnen de organisatie worden genormeerd. Dit zal de objectiviteit van de geformuleerde eisen vergroten.

## KWETSBAARHEIDSANALYSE

Na het uitvoeren van de afhankelijkheidsanalyse heeft men de betrouwbaarheidseisen voor het informatiesysteem of het verantwoordelijkheidsgebied geformuleerd. Op basis van de betrouwbaarheidseisen alleen is het echter nog niet mogelijk te komen tot een adequaat pakket aan beveiligingsmaatregelen. Bij de keuze van beveiligingsmaatregelen moet ook rekening worden gehouden met de dreigingen die de storingen in de informatievoorziening veroorzaken. Daarom zal men eerst de relevante bedreigingen moeten identificeren.
Het bepalen hiervan is een onderdeel van de kwetsbaarheidsanalyse.[19]

Bij het uitvoeren van een kwetsbaarheidsanalyse worden de volgende stappen doorlopen:

*Stap K1 – Inventarisatie relevante bedreigingen*
De eerste stap in de kwetsbaarheidsanalyse is het inventariseren van de dreigingen die van toepassing kunnen zijn in de te onderzoeken situatie. Vervolgens worden de relevante dreigingen gekoppeld aan de in de afhankelijkheidsanalyse geïnventariseerde IT-componenten. Door de enorme hoeveelheid mogelijke dreigingen te groeperen wordt de inventarisatie ervan beter hanteerbaar gemaakt. Bij de inventarisatie van mogelijke bedreigingen voor de onderkende componenten blijkt dat er bijna altijd sprake is van een n : m-relatie tussen IT-componenten en bedreigingen (zie figuur 3). Bij de koppeling van de bedreigingen aan de IT-voorzieningen wordt bovendien aangegeven welke invloed de dreiging heeft op de IT-component[20] en daardoor op de kwaliteit van de informatievoorziening.
Deze complexe verbanden vergen een zeer arbeidsintensieve administratie.

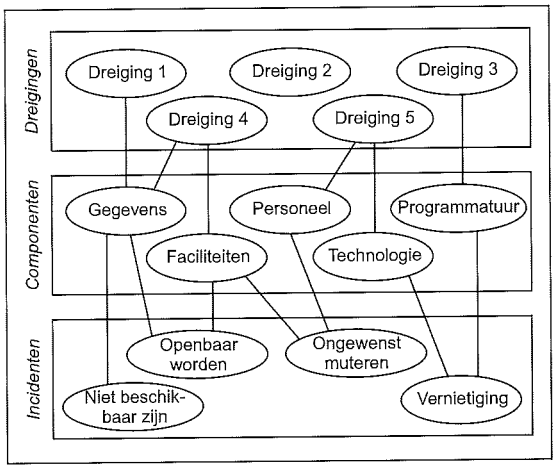
*Stap K2 – Inventarisatie van de kans op optreden van een bedreiging en ernst van gevolgen (gevoeligheid) hiervan*
De betrouwbaarheidseisen die zijn geformuleerd op grond van de afhankelijkheidsanalyse zijn opgesteld zonder rekening te houden met mogelijke dreigingen. De noodzakelijke beveiligingsmaatregelen zijn echter niet alleen afhankelijk van de geformuleerde betrouwbaarheidseisen. Ook de kans dat een dreiging optreedt en de omvang van de consequenties van het optreden spelen bij de selectie van maatregelen een rol. Daarom zullen de, in de afhankelijkheidsanalyse geformuleerde, eisen nog moeten worden verfijnd om op een verantwoorde wijze te komen tot een selectie van maatregelen. Een betrouwbaarheidseis heeft als het ware bandbreedte. Binnen deze bandbreedte moet positie worden gezocht. De kans dat een dreiging zich manifesteert en de ernst (omvang) van de gevolgen van het manifest worden van de dreiging zullen mede bepalend zijn voor de keuze van de aard van de maatregelen. De kans op optreden en de ernst van de gevolgen van de dreiging zijn (mede) bepalend voor de keuze van het moment dat een maatregel actief moet zijn.
De verbanden zijn aangegeven in tabel 2.

| *Kans* / *Ernst* | Groot | Klein |
|---|---|---|
| Groot | preventieve maatregelen | preventieve/ detectieve maatregelen |
| Klein | preventieve/ detectieve maatregelen | detectieve maatregelen |

*Tabel 2. Relatieschema dreigingen – maatregelen.*

Niet in deze tabel opgenomen zijn de repressieve en correctieve maatregelen die altijd in combinatie met detectieve maatregelen zullen moeten worden genomen.
Naast de kans en de ernst van een dreiging heeft ook de storing in de kwaliteit van de informatievoorziening invloed op de keuze van de aard van de maatregelen. Zo zal er bij eisen wat betreft exclusiviteit een voorkeur zijn voor preventieve maatregelen. Bij integriteit daarentegen kunnen detectieve maatregelen een voldoende waarborg zijn.

*Stap K3 – Selectie van maatregelen*
Op basis van de gevonden betrouwbaarheidseisen en de aangebrachte verfijning kunnen te selecteren beveiligingsmaatregelen worden vastgesteld. De te kiezen maatregelen moeten een zodanig stelsel vormen dat zij kunnen waarborgen dat aan de geformuleerde betrouwbaarheidseisen voor de informatievoorziening wordt voldaan. Hierbij moet 'aantoonbaar' zijn dat de gekozen maatregelen op elk moment van dien aard zijn dat aan de betrouwbaarheidseisen, rekening houdend met de kans en




*Figuur 3. Relatie IT-componenten – dreigingen.*

de ernst van de mogelijke dreiging, kan worden voldaan.
De keuze van maatregelen is een complex geheel. Dit wordt veroorzaakt door een n : m-relatie tussen de bedreigingen en de maatregelen. Een eis kan meerdere maatregelen in combinatie vereisen, andersom kan een maatregel bijdragen tot voorkomen van het manifest worden van meer dan één bedreiging of het beperken van de gevolgen daarvan.
Voor het maken van een verantwoorde selectie van beveiligingsmaatregelen om te kunnen voldoen aan de eisen wat betreft een betrouwbare informatievoorziening is het van belang rekening te houden met de kenmerken van beveiligingsmaatregelen. Een hulpmiddel hierbij kan zijn een groepering van de maatregelen naar verschillende gezichtspunten.[21]
Het ordenen van alle mogelijke maatregelen en deze maatregelen voorzien van de nodige kenmerken is een zeer arbeidsintensieve aangelegenheid. Bovendien zal men komen tot een zeer omvangrijk overzicht.
Een overzicht met alle mogelijke maatregelen en bijbehorende kenmerken is noodzakelijk bij het opstellen van alle beveiligingsplannen om een verantwoorde selectie te kunnen maken. Omdat praktisch niet verwacht mag worden dat elke lijnmanager zelfstandig alle mogelijke maatregelen limitatief bedenkt, is het raadzaam dit eenmalig op één centrale plaats binnen de organisatie te doen. Deze centrale instantie dient dan bovendien met het onderhoud van de maatregelen te worden belast.

De beveiligingsmaatregelen moeten zodanig worden gekozen dat er sprake is van een 'adequate' beveiliging, dit wil zeggen dat de beveiligingsmaatregelen, rekening houdend met de implementatiekosten ervan, overeenstemmen met het vereiste betrouwbaarheidsniveau.
Als zou blijken dat een evenwichtig pakket maatregelen niet mogelijk is, zal men het afschaffen van het systeem in overweging kunnen nemen. Hierbij zou men na moeten gaan in hoeverre het systeem noodzakelijk is voor het uitvoeren van het bedrijfsproces. (Hierbij kan een parallel worden getrokken met een onbeveiligde overweg: de kans op ongelukken (dreiging) is groot, het treffen van maatregelen is echter kostbaar, dus sluit men de overweg af.)

**Beveiligingsplan**

Door het uitvoeren van de in deze paragraaf genoemde stappen is men gekomen tot een beveiligingsplan. Daar aan de beveiligingsmaatregelen een 'waarde' is toegekend rekening houdend met het werkingsgebied, de effectiviteit, de aard en de implementatiekosten is gewaarborgd dat er, in overeenstemming met de voorwaarde gesteld in VIR94, sprake is van een evenwichtig pakket maatregelen.

Daarnaast wordt ook aan de voorwaarde voldaan dat het gekozen stelsel van informatiebeveiligingsmaatregelen op ieder moment zodanig dient te zijn dat aangetoond kan worden dat aan de betrouwbaarheidseisen wordt voldaan (VIR94).

Door het vastleggen van de resultaten van de stappen van zowel de afhankelijkheidsanalyse als de kwetsbaarheidsanalyse in tabellen en overzichten is het mogelijk uitgaande van het gevonden stelsel van informatiebeveiligingsmaatregelen terug te zoeken welke betrouwbaarheidseisen (gedeeltelijk) worden afgedekt door een specifieke maatregel. Door een n : m-relatie tussen maatregelen en dreigingen zal dit echter een erg complex verhaal zijn.
Ook zal, door snelle technologische ontwikkelingen op het gebied van de informatievoorziening, het eenmaal opgestelde beveiligingsplan geen statisch geheel kunnen zijn. Periodiek dient het plan te worden aangepast aan de veranderde omstandigheden. Een goede onderhoudbaarheid van een beveiligingsplan is daarom vereist.

## GEAUTOMATISEERDE HULPMIDDELEN

De verantwoordelijkheid voor het opstellen van een informatiebeveiligingsplan is gelegd bij de lijnmanagers. Deze functionarissen hebben doorgaans geen of weinig ervaring met het opstellen van zo'n plan. Het verdient daarom aanbeveling de methodiek voor het opstellen van een beveiligingsplan op een zo eenvoudig mogelijke wijze hanteerbaar te maken voor de lijnmanagers.

De intensieve administratie van de diverse verbanden en de bewerkelijkheid van de selectie van maatregelen maken het uitvoeren van de afhankelijkheidsanalyse en de kwetsbaarheidsanalyse tot een complex geheel. Het doorlopen van alle stappen is echter noodzakelijk om op een goed onderbouwde wijze te komen tot een stelsel van informatiebeveiligingsmaatregelen dat in evenwicht is met het belang van het informatiesysteem of verantwoordelijkheidsgebied voor de betrokken bedrijfs- of bestuursprocessen.
Het eenmalig leveren van deze zware inspanning voor het uitvoeren van deze analyses kan al bijna niet worden verwacht van de lijnmanagers. De noodzakelijke onderhoudbaarheid van de informatiebeveiligingsplannen maakt het echter zo goed als onmogelijk de werkzaamheden handmatig uit te voeren. De ondersteuning van het gehele proces door een geautomatiseerd hulpmiddel is daarom zeer wenselijk.

Bij het uitvoeren van de A- en K-analyse moet een groot aantal relaties worden gelegd. Dit kan eenvoudiger worden uitgevoerd als de methodiek wordt ondersteund door een geautomatiseerd hulpmiddel. De vraag hierbij is of men gebruik kan maken van een reeds bestaand hulpmiddel of dat er een speciaal op de in VIR94 genoemde A- en K-analyse gebaseerd hulpmiddel moet worden ontwikkeld.

Een belangrijk uitgangspunt hierbij is dat per 1 januari 1997 voor alle informatiesystemen, dus zowel de per 1 januari 1995 bestaande systemen als de na deze datum ontwikkelde systemen, en verantwoordelijkheidsgebieden een informatiebeveiligingsplan moest zijn gerealiseerd.
Het zelf ontwikkelen van een geautomatiseerd in-

strument voor het uitvoeren van een A- en K-analyse zal zeer zeker enige maanden, dan wel enige jaren in beslag nemen. Gezien de tijdslimiet die is gesteld voor het opstellen van een beveiligingsplan, biedt dit op dit moment dan ook geen uitkomst. Resteert een onderzoek naar een geschikt instrument dat reeds op de markt beschikbaar is. In het beleidsdocument bij het Ministerie van Defensie wordt de methodiek CRAMM versie 3.0[22] aanbevolen voor het uitvoeren van de A- en K-analyse. Uit een nader onderzoek van CRAMM 3.0 komt naar voren dat de stappen die moeten worden doorlopen om te komen tot een evenwichtig stelsel beveiligingsmaatregelen voor een informatiesysteem of verantwoordelijkheidsgebied (A- en K-analyse) zoals is voorgeschreven in VIR94, door CRAMM 3.0 in voldoende mate worden ondersteund. De complexe relaties nodig voor de selectie van maatregelen wat betreft relevante dreigingen kunnen met behulp van de methodiek goed inzichtelijk worden vastgelegd. Noodzakelijke mutaties in het beveiligingsplan kunnen op eenvoudige wijze worden aangebracht en zichtbaar gemaakt. Ook levert de methodiek ondersteuning bij het beheer en onderhoud van de implementatie van de benodigde beveiligingsmaatregelen.
De methodiek is echter geënt op de Engelse overheid. Hierdoor zijn naast de algemeen geldende maatregelen, specifiek op de Engelse wet- en regelgeving betrekking hebbende maatregelen opgenomen. Bovendien is de methodiek slechts in de Engelse taal beschikbaar. Dit kan enigszins nadelig werken in het licht van de gebruikersvriendelijkheid. De in de methodiek gebruikte terminologie sluit niet één op één aan bij de terminologie van het VIR. De genoemde bezwaren kunnen echter worden ondervangen zodra er voldoende (potentiële) Nederlandse gebruikers zijn. De methodiek kan dan worden aangepast aan de Nederlandse situatie.

## CONCLUSIES

De conclusies zijn zowel gericht op informatiebeveiliging als op de A- en K-analyses.

### Informatiebeveiliging

Informatiebeveiliging is een onderwerp waarover veel wordt gepraat, maar praatjes vullen geen gaatjes. De noodzaak tot het daadwerkelijk beveiligen wordt in veel gevallen pas duidelijk indien er een incident optreedt. Door de steeds belangrijkere rol die informatiesystemen zijn gaan spelen bij het uitvoeren van bedrijfs- en bestuursprocessen wordt de beveiliging van deze systemen echter steeds noodzakelijker. Het, op grond van wettelijke voorschriften, opstellen van een beveiligingsplan is echter geen afdoende middel om de informatiesystemen goed te beveiligen. Personen die op de een of andere manier betrokken zijn bij een informatiesysteem moeten zich bewust zijn van het belang van het informatiesysteem en dus het belang van de goede werking hiervan. Men moet het belang van de implementatie van beveiligingsmaatregelen inzien. Naast het opstellen van een beveiligingsplan zal binnen de organisatie daarom veel aandacht besteed moeten worden aan het bewustwordingsproces bij de bij een informatiesysteem betrokken personen.

Informatiebeveiliging moet echter niet worden gezien als een losstaand onderwerp. Zij zal een onderdeel moeten gaan vormen van de gehele kwaliteitszorg. Al bij het ontwerp en de bouw van een informatiesysteem moet rekening worden gehouden met de beveiliging. Zij moet bovendien aansluiten bij het algemene beveiligingsbeleid van de organisatie. Veel maatregelen die noodzakelijk zijn bij informatiebeveiliging zijn immers ook noodzakelijk bij de beveiliging in het algemeen. De informatiebeveiliging moet dus ingebed worden in de organisatie en hierin een vanzelfsprekend aandeel vormen. Dit houdt onder meer in dat het onderhoud van de opgestelde (informatie)beveiligingsplannen en de implementatie van de beveiligingsmaatregelen periodiek worden gecontroleerd en zo nodig worden aangepast aan de (gewijzigde) omstandigheden.

### Afhankelijkheids- en kwetsbaarheidsanalyse

In het geheel genomen is CRAMM 3.0 een goed en bruikbaar instrument voor het uitvoeren van een A- en K-analyse. De resultaten van de analyses zijn, door de diverse tabellen en geautomatiseerde relaties in CRAMM 3.0, objectief en reproduceerbaar. Het verdient echter aanbeveling de in de methodiek gehanteerde terminologie en de hierin opgenomen wet- en regelgeving aan te passen aan de Nederlandse omstandigheden. De eerste stappen hiertoe zijn inmiddels gezet. Op zeer korte termijn wordt een Nederlandstalige versie van CRAMM 3.0 verwacht. Dit zal de gebruikersvriendelijkheid en daardoor de acceptatiegraad van de gebruikers verhogen.
Het handmatig uitvoeren van de A- en K-analyse is gezien de complexiteit en de gebrekkige onderhoudbaarheid hiervan sterk af te raden.

## NOTEN

*1. Computerbeveiliging. Beveiliging van gegevens in geautomatiseerde systemen bij de ministeries, brief van de Algemene Rekenkamer. Tweede Kamer der Staten-Generaal, vergaderjaar 1988-1989, 20 904, nrs. 1-2, 's-Gravenhage 1988.*

*2. Technologische ontwikkelingen hebben onder meer tot gevolg dat de gebruikte apparatuur steeds kleiner wordt, dat de opslagcapaciteit steeds groter wordt en dat bewerkingen in steeds kortere tijd kunnen worden uitgevoerd. Dit leidt tot een steeds verdere decentralisatie. Apparatuur, programmatuur en gegevens kunnen op veel werkplekken in de organisatie worden geplaatst. De geautomatiseerde informatieverwerking is niet meer het exclusieve werkgebied van gespecialiseerde organisatie-eenheden. Overal binnen de organisatie wordt gebruikgemaakt van geautomatiseerde informatieverwerking. De genoemde technologische ontwikkelingen maken het bovendien mogelijk de diverse informatiesystemen te koppelen. Hierdoor zijn gegevens steeds eenvoudiger te benaderen maar worden de gegevensstromen steeds moeilijker beheersbaar.*

*3. Hierbij kan worden gedacht aan onder andere verzelfstandiging, integraal management en zelfbeheer.*

*4. Bijvoorbeeld een geclassificeerd gegevensbestand, waarbij de beveili-*

*Mw. drs. M.C.C. van der Burg RI*
*Is als EDP-auditor werkzaam bij de Controle Sector EDP-auditing van de Defensie Accountantsdienst. Informatiebeveiliging vormt een belangrijk aandachtsgebied binnen haar werkzaamheden.*

*J.M.W. van de Garde RE*
*Is luitenant-kolonel bij de Koninklijke Luchtmacht en als EDP-auditor werkzaam bij de Controle Sector EDP-auditing van de Defensie Accountantsdienst.*

*ging specifiek is gericht op de exclusiviteit.*
*5. Ministerie van Binnenlandse Zaken. Voorschrift Informatiebeveiliging Rijksdienst, Den Haag 1994.*
*6. Een geheel van voorzieningen dat ter beschikking staat aan één of meer informatiesystemen en waarvoor de verantwoordelijkheid eenduidig is toe te wijzen aan één organisatorische eenheid, bijvoorbeeld een lokaal netwerk.*
*7. Evenwichtig betekent dat een balans bestaat tussen de kosten en lasten van (extra) maatregelen enerzijds en de baten in de vorm van vermeden risico's anderzijds (VIR94). De Wet Computer Criminaliteit (WCC) spreekt in dit geval van een adequate beveiliging. In de Memorie van Toelichting bij de Wet Computer Criminaliteit wordt onderscheid gemaakt tussen absolute, maximale, adequate, minimale en proformabeveiliging (K.IJ. Mollema, H. Franken, A.H.M. de Groot, J. Pasmooij en A.J.M. Werring, Computercriminaliteit, de wetgeving, de gevolgen voor bedrijven en de accountant. NIVRA-geschrift 62, Automatisering en controle, Deel IX, Amsterdam 1993).*
*8. Onder risicoanalyse wordt verstaan:*
- *het systematisch inventariseren van de bedreigingen waaraan een proces onderworpen kan zijn;*
- *het inschatten van de kansen (kansberekening) op het optreden van de dreiging en het inschatten van de mogelijke gevolgen van het blootstellen van het proces aan die bedreigingen;*
- *het doen van voorstellen om die gevolgen te minimaliseren op basis van de in het beveiligingsbeleid aangegeven uitgangspunten (Risico-analyse en risicomanagement, Nederlands Genootschap voor Informatica, Afdeling Beveiliging, 1992).*

*9. Een afhankelijkheidsanalyse is het vaststellen in hoeverre bestuurs- en bedrijfsprocessen die door een informatiesysteem worden ondersteund, afhankelijk zijn van de betrouwbaarheid van dit systeem en welke potentiële schaden kunnen optreden als gevolg van een verstoring van de informatievoorziening.*
*10. Enkele voorbeelden van storingen in de informatievoorziening die gevolgen kunnen hebben voor het bedrijfsproces zijn: gegevens uit het bedrijfsproces kunnen niet of niet op integere wijze vastgelegd, zijn niet op het juiste moment beschikbaar of zijn bij te veel of de verkeerde personen bekend geraakt.*
*11. In een beveiligingsplan moet worden vastgelegd welke informatiebeveiligingsmaatregelen van kracht zijn voor een informatiesysteem of een verantwoordelijkheidsgebied.*
*12. W. Hartman, Het ontwerpen van informatiesystemen, een inleiding, 4e druk, Deventer 1986.*
*13. De gegevens (gebeurtenissen) in de werkelijke situatie (het bedrijfsproces en de omgeving) moeten worden vastgelegd in een informatiesysteem.*
*14. De informatie uit het informatiesysteem naar het reële systeem (bedrijfsproces) wordt gebruikt voor aansturing van de bedrijfs- of bestuursprocessen. Informatiesystèmen zijn daardoor een belangrijk middel voor het bereiken van de doelstelling van de organisatie. De aansturing van het reële informatiesysteem kan worden beïnvloed als de in het informatiesysteem opgenomen gegevens (onbedoeld) bekend worden bij de omgeving en tot een reactie van die omgeving leiden die van invloed is op het desbetreffende reële systeem of een ander reëel systeem.*
*15. Een bedreiging is een situatie die kwalijke gevolgen in het vooruitzicht stelt (G. Geerts en H. Heestermans, m.m.v. C. Kruyskamp, Van Dale Groot woordenboek der Nederlandse taal, 11e, herziene druk).*
*16. Een voorbeeld van een mogelijke dreiging is brand. Als er daadwerkelijk brand uitbreekt, kan hierdoor het mainframe (IT-voorziening) worden verwoest. Een voorraadadministratie van onderdelen bij een defensie-onderhoudswerkplaats (informatiesysteem) die onder andere met behulp van dit mainframe wordt bijgehouden, kan gedurende een bepaalde periode niet worden benaderd. Hierdoor kan de tijdige levering van onderdelen voor herstel van materieel worden vertraagd, waardoor het voertuig mogelijk tijdelijk niet inzetbaar is (potentiële schade). Hoe meer voertuigen niet inzetbaar zijn, hoe meer ongenoegen binnen operationele eenheden zal ontstaan en hoe waarschijnlijker het is dat men elders de reparatie laat uitvoeren, waardoor omzetverlies ontstaat (scenario).*
*17. De gevolgen van storingen in het informatiesysteem of het verantwoordelijkheidsgebied voor de informatie/gegevens zijn, gezien in relatie met de eerdergenoemde kwaliteitscriteria, globaal in een drietal groepen in te delen, te weten:*
- *de informatie is niet beschikbaar (gedurende een bepaalde periode) (beschikbaarheid);*
- *de informatie is ongeautoriseerd gewijzigd, dat wil zeggen is niet (meer) in overeenstemming met de werkelijkheid (integriteit);*
- *de informatie is ongewenst openbaar geworden (exclusiviteit).*

*18. Een bedreiging is een proces dat in potentie verstorend is voor één of meer onderdelen van een organisatie (M.E.M. Spruit en dr. ir. M. Looijen, Beveiliging van informatievoorziening, onderzoek op basis van landelijke enquête '93-'94, Delft 1994).*
*19. Een kwetsbaarheidsanalyse is het vaststellen van de invloed van het manifest worden van bedreigingen op het functioneren van een informatiesysteem of van een verantwoordelijkheidsgebied.*
*20. Disfunctioneren, storing of beschadiging van het middel. De invloed van het disfunctioneren, de storing of de beschadiging van de desbetreffende IT-component op de kwaliteit van de informatievoorziening wordt hier ook aangegeven.*
*21. In de literatuur (Gemeente Amsterdam, Handboek Informatiebeveiliging, Amsterdam 1994; Nederlands Normalisatie-instituut en Ministerie van Economische Zaken, Code voor informatiebeveiliging, een leidraad voor beleid en implementatie, Delft 1994; Checklist Computerbeveiliging, Nederlands Genootschap voor Informatica, sectie Beveiliging, 1987; Beveiligingsvoorschrift G-geheel Departement Defensie (VGVK 23), 's-Gravenhage) is een aantal overzichten te vinden met mogelijke beveiligingsmaatregelen. Deze overzichten kunnen worden gebruikt als een geheugensteun bij de keuze van maatregelen. Het blijft echter, ook met behulp van deze overzichten, nauwelijks mogelijk de volledigheid van de maatregelen vast te stellen.*
*Om tot een evenwichtige keuze van maatregelen te kunnen komen zal men daarom alle mogelijke beveiligingsmaatregelen moeten ordenen. Bij elke beveiligingsmaatregel moet worden aangegeven wat de kosten van implementatie zijn, de aard, de werkingssfeer en de effectiviteit. Bovendien moet worden aangegeven tegen welke bedreiging(en) de maatregel effectief is en in welke mate.*
*Daarnaast is het zinvol bij de maatregel aan te geven tot welk betrouwbaarheidsaspect de implementatie van de maatregel zal bijdragen. Hierbij zal, om aansluiting te kunnen vinden bij de geformuleerde betrouwbaarheidseisen, een indeling aangehouden moeten worden die overeenstemt met de bij de afhankelijkheidsanalyse geformuleerde niveaus. Een aantal indelingen van maatregelen is:*
***Maatregelen naar hun aard***
*Bij deze indeling worden de maatregelen gerangschikt naar het moment van functioneren in relatie tot het optreden van een verstoring:*
- *reducerende maatregelen, gericht op het reduceren van de kans op het manifest worden van de dreiging;*
- *preventieve maatregelen, gericht op het voorkomen van verstoringen;*
- *detectieve maatregelen, gericht op het ontdekken van het optreden van verstoringen;*
- *repressieve maatregelen, gericht op het beperken van de schade;*
- *correctieve maatregelen, gericht op het herstellen van de schade;*
- *evaluerende maatregelen, gericht op de analyse van de toereikendheid van de geïmplementeerde maatregelen.*

*(P.L. Overbeek, Verleden, heden en toekomst van informatiebeveiliging: Invloed van veranderingen in de informatietechnologie, TNO-rapport FEL-91-B321, 1991.)*
***Maatregelen naar hun werkingssfeer***
*Hierbij worden de maatregelen onderscheiden naar het gebied waarin of waarvoor ze zijn getroffen:*
- *fysieke maatregelen;*
- *organisatorische en personele maatregelen;*
- *maatregelen in apparatuur en programmatuur;*
- *juridische maatregelen.*

*(Ministerie van Binnenlandse Zaken, Handboek Informatiebeveiliging Rijksdienst 1995, Den Haag 1995.)*
***Maatregelen naar hun effectiviteit***
*Daarnaast is het mogelijk de maatregelen in te delen naar het kwaliteits-*

*kenmerk waarop zij betrekking hebben:*
- *beschikbaarheid (continuïteit);*
- *integriteit;*
- *exclusiviteit.*

*(Ministerie van Binnenlandse Zaken, Handboek Informatiebeveiliging Rijksdienst 1995, Den Haag 1995.)*

*22. CCTA Risk Analyses and Management Method.*

# BIJLAGE

## Beschrijving CRAMM-methodiek

CRAMM is de afkorting voor CCTA Risk Analyses and Management Method. Het is een methodiek die niet alleen de risico's inventariseert en analyseert, maar bovendien ondersteuning biedt bij het beheersen van risico's.
De methodiek is ontwikkeld door CCTA (Central Computer and Telecommunications Agency) voor de Engelse overheid. Doordat het pakket is ontwikkeld voor de overheid worden specifieke overheidsbelangen meegenomen in de beoordeling en het management van risico's.
De methodiek kent een gefaseerde aanpak om tot een pakket beveiligingsmaatregelen te komen. De verschillende fasen van de methodiek zullen hierna worden beschreven. In CRAMM is een drietal fasen te onderkennen. Deze fasen moeten volgtijdig worden doorlopen.
In de eerste fase kan een aantal basisgegevens van het systeem worden beschreven. Hier kan door middel van vrije tekst onder meer worden aangegeven waar de grenzen van het te onderzoeken systeem zijn gelegd. Bovendien kan hier de relatie tussen bedrijfs- en bestuursprocessen enerzijds en informatiesystemen anderzijds worden aangegeven. Deze informatie heeft een functie bij de documentatie van het onderzoek maar wordt niet gebruikt bij de keuze van de benodigde beveiligingsmaatregelen in de derde en laatste fase.
In deze eerste fase vindt bovendien identificatie en waardebepaling plaats van de in het systeem opgenomen componenten. De componenten worden onderscheiden in:
- data (gegevens(verzamelingen));
- programmatuur (standaardpakketten en maatwerk);
- fysieke componenten.

Bij de identificatie van de programmatuur en de fysieke componenten dient een typering te worden aangegeven. De mogelijke typeringen zijn opgenomen in een uitgebreid, maar uitputtend overzicht. Het aangeven van de typering is noodzakelijk met het oog op de mogelijke dreigingen en de selectie van noodzakelijke maatregelen in de derde fase.
De waardering van alle componenten wordt uitgedrukt in een cijfer op een schaal van één tot tien. De waardering van de fysieke componenten is, voorzover van belang, gebaseerd op vervangingswaarde.
Als de vervangingswaarde kunnen worden genomen de kosten die gemaakt moeten worden indien de desbetreffende component opnieuw moet worden aangeschaft en geïnstalleerd (kosten van herinvesteringen en reconstructie). De geldswaarden worden door het geautomatiseerde instrument omgezet in een cijfer.
De gegevens en de programmatuur worden gewaardeerd tegen de gebruikswaarde die is gebaseerd op de potentiële schade voor de organisatie door vernietiging (vanaf of inclusief de laatste back-up), niet beschikbaar zijn (gedurende een aantal kritische termijnen), al dan niet opzettelijk (ongeautoriseerd) wijzigen of ongewenst openbaar worden. Deze potentiële schade wordt verkregen uit interviews met de eigenaar (meest belangrijke gebruiker) van een component. De verslagen van de interviews en de op deze wijze verkregen gebruikswaarde moeten worden vastgelegd met behulp van de ondersteunende programmatuur. De handleiding bij de methodiek en de in de programmatuur opgenomen helpinformatie geven een richtlijn voor de waardering van bepaalde schadescenario's (valuation guidelines). Hierdoor wordt de objectiviteit van de waardering vergroot.

Tot de fysieke componenten worden in de methodiek gerekend die componenten die niet vallen onder gegevens of programmatuur, bijvoorbeeld:
- computerapparatuur (printers, mainframe, terminals, etc.);
- verbindingsapparatuur (clustercontrollers, etc.);
- infrastructuur (LAN, WAN, etc.);
- end-userservice (dienst die ter beschikking staat van de eindgebruiker, bijvoorbeeld e-mail);
- communicatieprotocollen.

Per fysieke component moeten de kenmerken en, indien relevant, de vindplaats hiervan worden aangegeven.

Programmatuur kan worden onderverdeeld naar de soort informatie die hiermee wordt verwerkt (bijvoorbeeld logistieke systemen, financiële systemen, beveiligingssystemen, etc.). Bovendien moet bij de programmatuur worden aangegeven of het een standaardpakket is dan wel maatwerk (al dan niet vertrouwelijk). De waardering van beide soorten programmatuur gebeurt op dezelfde wijze. De besturingsprogrammatuur maakt deel uit van de fysieke component en wordt niet afzonderlijk gewaardeerd.
Gegevenselementen in het afgebakende gebied (informatiesysteem, verantwoordelijkheidsgebied) worden gewoonlijk niet afzonderlijk beoordeeld maar samengevoegd tot logische eenheden (gegevensgroepen).
De relatie tussen de diverse componenten moet door de gebruiker worden aangegeven. Deze relaties worden vastgelegd in het 'assetmodel'. Het uitgangspunt hierbij zijn de (logische) gegevensgroepen met daaraan gekoppeld de end-userservices.
Op grond van de nu geïnventariseerde componenten en de bijbehorende waarde en de onderlinge relaties tussen de verschillende componenten berekent de programmatuur de uiteindelijke waarde van de componenten. Dit zijn de betrouwbaarheidseisen voor de afzonderlijke componenten.
Bij het berekenen van de waarde van de diverse groepen wordt rekening gehouden met de gedefinieerde afhankelijkheden. De hoogste waarde van

de gerelateerde componenten bepaalt uiteindelijk de waarde van de groep. In het 'backtrackoverzicht' wordt zichtbaar op grond van welke redenering men is gekomen tot de desbetreffende waardering (betrouwbaarheidseisen).

In de tweede fase worden de componenten, zoals benoemd in de eerste fase, gegroepeerd. Het doel van deze groepering is het beperken van de in deze fase te beantwoorden vragenlijsten. Er moet per (groep) component(en) voor elke relevante dreiging een tweetal vragenlijsten worden beantwoord. Indien men componenten die blootstaan aan dezelfde dreiging samenvoegt kan men volstaan met het beantwoorden van de vragenlijsten voor de gehele groep. Een in de eerste fase gedefinieerde component kan worden opgenomen in meerdere groepen. De beantwoording van de eerste vragenlijst moet een inzicht geven in de kans dat de dreiging manifest wordt. Deze kans wordt weergegeven in termen van zeer hoog, hoog, gemiddeld, laag of zeer laag. De tweede vragenlijst moet inzicht geven in de kwetsbaarheid (gevoeligheid) van de organisatie als een dreiging zich voordoet. Dit wordt uitgedrukt in hoog, gemiddeld of laag. De vragenlijsten bestaan uit een relatief klein aantal multiple-choicevragen, die vrij eenvoudig beantwoord kunnen worden. In de handleiding bij de methodiek CRAMM 3.0 is een bijlage opgenomen die hulp biedt bij het koppelen van dreigingen aan componenten. Op basis van de, in de eerste fase gevonden, waarde en de, met behulp van de vragenlijsten uit de tweede fase gevonden, kans en kwetsbaarheid zal door de programmatuur een overzicht worden gegenereerd met het risiconiveau en dus het benodigde beveiligingsniveau.

Nadat aan het eind van de tweede fase het beveiligingsniveau is berekend, worden in de laatste fase de gedetailleerde beveiligingsmaatregelen geselecteerd uit een database. Dit is een proces dat door de programmatuur wordt uitgevoerd. Bij de geselecteerde maatregelen wordt aangegeven:
- de aard van de maatregelen;
- de werkingssfeer;
- de implementatiekosten (in termen van hoog, gemiddeld en laag);
- het beveiligingsniveau waartoe de maatregel bijdraagt.

Bij de geadviseerde maatregelen kan door de gebruiker worden aangegeven of deze al dan niet geïmplementeerd zijn. Indien implementatie van de maatregelen nog niet heeft plaatsgevonden, kan worden aangegeven wat de organisatie van plan is met de geadviseerde maatregel. De argumentatie met betrekking tot de beslissing over de implementatie van de geadviseerde maatregel kan worden gedocumenteerd bij de betrokken maatregel. Hierdoor is te allen tijde een audit trail beschikbaar.

In de derde fase van CRAMM is tevens een what-if-functie opgenomen. Met behulp van deze functie kunnen de gevolgen voor de beveiliging als gevolg van wijzigingen in het onderzochte systeem snel zichtbaar worden gemaakt. De wijzigingen in het systeem kunnen betrekking hebben op alle in de eerste en tweede fase ingevulde gegevens. Wijzigingen in de maatregelen worden als zodanig gemarkeerd. Daar in veel situaties sprake is van technologische ontwikkelingen en/of een veranderend inzicht in de wijze waarop organisaties moeten worden aangestuurd, biedt deze functie een belangrijke steun bij het onderhoud van de beveiligingsplannen.

CRAMM is een pakket dat in Engeland veel wordt gebruikt bij de overheid. De gebruikers van het pakket zijn verenigd in een zeer actieve User Group. De User Group onderhoudt nauwe banden met de ontwikkelaars van het systeem. Hierdoor kan het pakket regelmatig worden aangepast aan nieuwe ontwikkelingen en wensen van gebruikers. Er is inmiddels ook een Nederlandse aanbieder van het pakket. Deze aanbieder kan in Nederland de helpdesk-functie vervullen. Bovendien zal op korte termijn een Nederlandstalige versie van het pakket verschijnen. Door het toenemende gebruik van CRAMM in Nederland wordt eraan gedacht een Nederlandse gebruikersgroep op te richten, zodat de specifieke Nederlandse belangen kunnen worden ondergebracht in de methodiek. De beheersorganisatie rond het pakket is dus goed geregeld.

*Overzicht mogelijke schaden opgenomen in CRAMM-methodiek*
- Persoonlijke veiligheid;
- privacy (persoonlijke informatie);
- wet- en regelgeving;
- wetsovertreding;
- commercieel en economisch belang;
- financieel verlies/verstoring bedrijfsactiviteiten;
- openbare orde;
- internationale relaties;
- defensie/operationele inzetbaarheid;
- veiligheid en inlichtingen;
- beleid en uitvoeren van overheidstaken;
- verlies goodwill.

# Audit en beheer van Jaar 2000-projecten

Prof. W. Van Grembergen

**Het Jaar 2000-probleem is ontstaan doordat informatiesystemen die de laatste dertig jaren werden ontwikkeld, gebruikmaken van slechts twee posities om het jaartal te specificeren. Dit zal een groot probleem worden wanneer de 21ste eeuw zal worden bereikt. Deze bijdrage stelt een formele benadering voor om dit belangrijke IT-onderhoudsproject te beheersen en te auditen. De benadering is gebaseerd op CobiT, een recent ontwikkeld IT-audit- en controlemodel dat werd uitgebreid en gedetailleerd met elementen van Jaar 2000-publicaties.**

## INLEIDING

Het Jaar 2000 (Y2K)-probleem, in de Angelsaksische publicaties bekend als *Millennium Bug, Data Change Problem, Millennium Conversion, Century Compliance Problem,* en combinaties van deze termen, is een zeer actueel thema in organisaties. Het probleem is toe te schrijven aan het feit dat computersystemen meestal twee posities (97 in plaats van 1997) gebruiken om data voor te stellen. Zelfs nu doen zich in dit verband reeds problemen voor met applicaties zoals hypothecaire leningen die te maken hebben met toekomstige vervaldagen. Er waren bijzonder goede redenen voor deze datumvoorstelling met slechts twee karakters: het beperken van het aantal toetsaanslagen en besparingen inzake dure opslagmedia. Bovendien werd aangenomen dat de levensduur van de meeste toepassingen voor het jaar 2000 ten einde zou zijn. De realiteit is evenwel anders en heel veel systemen van het eerste uur zullen ook nog na het magische jaar 2000 in gebruik zijn. Dit betekent dat een groot aantal computersystemen moet worden aangepast aan het jaar 2000 (de systemen moeten *year 2000 compliant* zijn), wat een op zich eenvoudig maar terzelfdertijd complex probleem is.

Ondanks het feit dat sommige bedrijfsorganisaties reeds gestart zijn met het oplossen van dit probleem, is het eigenlijk pas sinds kort dat het grote aandacht krijgt. Het Y2K-fenomeen is zelfs een populair onderwerp geworden voor ontelbare seminars en congressen en is een levendig onderwerp op Internet met websites zoals De Jagers *Year 2000 Information Center (http://www.year2000.com/).* Vandaag trachten meer en meer organisaties de kosten van een Y2K-project te schatten en ze verkondigen dat heel wat geld zal moeten worden geïnvesteerd in deze conversie. Een belangrijke Belgische bank heeft berekend dat haar omschakeling ongeveer 33 miljoen US dollars zal kosten.

Het Y2K-project is een uniek project ([Jage96a]): de leveringsdatum moet absoluut worden gehaald, kan niet worden uitgesteld ook wanneer het gaat om zeer grote installaties, en geldt voor alle organisaties. Deze kenmerken zijn ook de redenen waarom een Y2K-project zeer risicicovol is en moet worden uitgevoerd op een beheerste manier. Met andere woorden: een Y2K-project is een onderhoudsproject dat moet worden gerealiseerd op basis van juiste structuren, procedures en praktijken.

Dit artikel onderzoekt dan ook de beheerobjectieven en beheersmaatregelen betreffende het Y2K-project. Het is de verantwoordelijkheid van het bedrijfsmanagement om deze conversie te beheersen. Managers hebben daarbij behoefte aan een raamwerk van gestandaardiseerde of algemeen geaccepteerde Y2K-controlepraktijken. Op basis van het CobiT-model en website-publicaties wordt hierna een beheer- en auditmodel beschreven. Het CobiT-model werd recentelijk ontwikkeld door leden van de Information Systems Control and Audit Association (ISACA, voorheen EDPAA), de leidende beroeps-IT-organisatie ([ISAC96a]), ([ISAC96b]).

## DE MILLENNIUM-CONVERSIE

Voor de goede orde wordt hier een overzicht gegeven van de oorzaken van de problemen.

### Het Y2K-fenomeen

Zoals hiervoor aangegeven, is de oorzaak van het Y2K-probleem de voorstelling van de jaarcode in twee posities. In COBOL-programma's bestaat het traditionele dataformaat uit zes karakters: JJMMDD of DDMMJJ. Bij het bereiken van het jaar 2000 resulteert dit in de volgende problemen:

- *Overflow:* 991231 + 1 dag wordt 000101 (1 januari 2000).
- Negatief aantal jaren: een persoon geboren in 1947 wordt in het jaar 2000 (00–47) = –47 jaar of – in het geval de programmeur een absolute waarde berekent – 47 jaar, wat een moeilijker te detecteren fout is.
- Incorrecte sortering: 00,01,47,49,83,84,99.
- 00 en 99 worden door programma's vaak herkend als uitzonderingsgevallen (00 bijvoorbeeld kan betekenen dat de geboortedatum niet bekend is of niet werd opgegeven).

Bovendien is het jaar 2000 niet alleen een tijdbom omdat het een overgang is naar een nieuw millennium, maar ook omdat het een bijzonder schrikkeljaar is. (Een jaar is een schrikkeljaar indien het ofwel deelbaar is door 400 ofwel deelbaar door 4 en niet door 100). Heel wat hardware- en softwareproducten zijn zich hier niet van bewust en zullen verkeerde data berekenen vanaf 29 februari 2000.

Het Y2K-probleem raakt niet alleen applicatiesoftware maar ook:

- alle hardwareplatformen: PC's, mini's, mainframes en netwerken;
- systeemsoftware zoals bedrijfssystemen, databasemanagementsystemen, telecommunicatiesoftware en programmeertalen;
- bestanden en databases met actuele en historische gegevens;
- formulieren en schermen;
- softwarepakketten.

### De technische Y2K-oplossingen

De twee meest populaire oplossingsstrategieën zijn de interpretatie en de expansie. Er bestaat een variëteit van termen die worden gebruikt om deze twee opties te beschrijven: procedurele versus data-aanpassing ([Eldr96]), en windowing-techniek versus volledige conversie ([IBM96]). Bij interpretatie wordt de programmalogica zodanig gewijzigd dat de twee datumposities worden geïnterpreteerd als een eeuw en een jaar. Eenvoudige algoritmen definiëren een afkapgrens: bijvoorbeeld 'voor 50' wordt vertaald naar de 21ste eeuw en '50' en 'na 50' wordt omgezet naar de 20ste eeuw (tabel 1).

De interpretatie is een eenvoudige oplossing en vereist alleen de aanpassing van de programma's; de tweecijferige jaarcodes hoeven niet te worden uitgebreid naar viercijferige formats, noch in de programma's, noch in de bestanden. Deze oplossing kan evenwel niet worden aangewend in het geval van geboortedata omdat een persoon geboren in 1901 dan zou zijn geboren in 2001.

Expansie is een meer fundamentele benadering: het betreft zowel de aanpassing van de programmacodes als van de bestanden en databases naar viercijferige jaardata (tabel 2).

In de praktijk wordt dikwijls voor een gemengde oplossing gekozen: waar mogelijk zal men zijn toevlucht nemen tot interpretatie omwille van kosten en tijdwinst, en expansie alleen kiezen wanneer het werkelijk nodig is. De beslissing zal sterk afhankelijk zijn van de ouderdom en de nog te verwachten levensduur van het systeem ([Eldr96]): een applicatie die nog een lange levensduur heeft, zal het meest profiteren van de uitbreidingsoplossing, terwijl een toepassing die binnenkort zal worden vervangen het best kan uithouden met de interpretatieve benadering.

Er kan geconcludeerd worden dat het Y2K-probleem technisch gezien een eenvoudige zaak is. Het is evenwel een bijzonder groot en tijdverslindend project omdat in alle programma's, bestanden en databases de millenniumproblemen moeten worden gedetecteerd en opgelost, wat het eigenlijk meer een plannings- en managementprobleem maakt. Het grote probleem ligt hierin dat alle plaatsen waar data verwerkt worden, moeten worden geïdentificeerd. Ondanks het feit dat er bij de uitvoering van deze conversietaak geautomatiseerde hulpmiddelen en software kunnen worden ingezet, zal er steeds een deel handmatig werk overblijven omdat sommige data verborgen zitten en/of moeilijk herkenbare namen hebben. Aangenomen

Bestaand programma

```
if JJMMDD1 is greater than JJMMDD2
```

Aangepast programma

```
if JJ is less than 50
        then move 20 to XX
        else move 19 to XX

if XXJJMMDD1 is greater than XXJJMMDD2
```

*Tabel 1. Interpretatie-oplossing: COBOL-voorbeeld.*

| Bestaand bestand | 2000-aangepast bestand |
|---|---|
| **970107** | **19970107** |
| Bestaand programma | 2000-aangepast programma |
| **02 JJMMDD picture 9(6)** | **02 JJJJMMDD picture 9(8)** |

*Tabel 2. Expansieoplossing: bestand en COBOL-programma.*

wordt dat de millenniumconversie één van de grootste onderhoudstaken is waarmee informatici ooit werden geconfronteerd.

**Het Y2K-project**

Het succes van een Y2K-project is sterk afhankelijk van het gebruik van een goede methodologie en goed projectmanagement. Wij stellen hier de volgende vijf fasen voor:
1. strategiedefinitie en inventarisatie;
2. budgettering;
3. impactanalyse;
4. ombouwen;
5. conversie en testen.

*1. Strategiedefinitie en inventarisatie*
Het algemeen management moet sterk betrokken zijn in het Y2K-project en moet een strategie bepalen aangaande de oplossing. Dit is reeds problematisch omdat het bedrijfsleven zich nog niet ten volle bewust is van de dimensie van het probleem. De Jager ([Jage96a]) onthult dat 65 procent van de Noord-Amerikaanse bedrijven nog niet begonnen is met de oplossing van dit probleem. Dit wordt bevestigd door de Belgische situatie: een aantal financiële bedrijven is reeds gestart met een Y2K-project, maar vooral de kleine en middelgrote ondernemingen zijn zich nog niet bewust van het Millenniumfenomeen en verwachten dat de IT-industrie pasklare oplossingen zal aanbieden. Organisaties moeten evenwel met gezwinde spoed starten met een dergelijk project teneinde uiterlijk op zaterdag 1 januari 2000 systemen te hebben die Y2K-conform zijn. De Jager ([Jage96b]) stelt dat het nu reeds te laat zou zijn wanneer men nog moet beginnen en beveelt een 'systematic triage' aan: het selecteren van die systemen die strategisch kritiek zijn en ten minste deze systemen Y2K-geschikt maken.

Een Y2K-strategisch plan bevat de volgende elementen:
- inventarisatie van de applicaties:
  - Welke applicaties zullen nog bestaan na het jaar 2000?
  - Welke applicaties moeten eerst worden aangepakt?
- technische inventarisatie:
  - Welke programmeertalen zijn in gebruik (COBOL, rekenbladen, ...)?
  - Zijn de source codes nog beschikbaar en waar kunnen ze worden gevonden?
  - Welke hardware- en systeemplatformen zijn in gebruik en zijn reeds Y2K-geschikt?
  - Wat is de kwaliteit van het configuratiemanagement?
  - Zijn er goede testprocedures en -praktijken in gebruik?
- inventarisatie van toepassingspakketten;
- reikwijdte:
  - Wordt alleen het Y2K-probleem opgelost of wordt ook van de gelegenheid gebruik gemaakt om het systeem te reengineeren?
  - Worden tegelijkertijd bestaande IT-problemen opgelost zoals het op scherp stellen van de testprocedures?
- de insourcing- en de outsourcingbeslissing;
- de selectie van consultant(s) en outsourcer(s);
- de keuze tussen interpretatie en/of expansie;
- de selectie van geautomatiseerde hulpmiddelen.

Sommige van deze componenten vergen enige toelichting en commentaar.

Het bepalen van het kritieke karakter van de verschillende applicaties en het voorrang geven aan het Y2K-conform maken zijn twee belangrijke activiteiten ([IBM96]). De wenselijkheid van de Y2K-omschakeling moet worden gebaseerd op de impact die het probleem heeft op de specifieke applicatie en op wat het belang is van de applicatie voor het bedrijf: een loonverwerkingssysteem dat uiteraard zeer gevoelig is voor een afgebroken en niet-tijdige verwerking wegens millenniumfouten, zal ongetwijfeld één van de eerste kandidaten zijn voor conversie.

Het is een zeer cruciale vraag of een applicatie al of niet reeds Y2K-aangepast is. Een manier om dit te weten te komen is contact op te nemen met de desbetreffende leverancier. Een Belgisch bedrijf nam dan ook contact op met zijn leveranciers van softwarepakketten en systeemsoftware. Het resultaat van dit experiment was zeer ontgoochelend: slechts enkelen lieten weten dat zij zich bewust zijn van het probleem en eraan werken, en meer dan vijftig procent gaf zelfs in het geheel geen antwoord.

*Outsourcing of uitbesteding is een attractief alternatief voor de oplossing van het Y2K-probleem.*

Outsourcing of uitbesteding is een attractief alternatief voor de oplossing van het Y2K-probleem. Een Belgische bank besliste om het technische Y2K-werk uit te besteden aan een softwarehuis in India. *Offshore* outsourcing is typisch geschikt in het geval van Y2K-onderhoud omdat het in essentie om een technisch probleem gaat. Dit specifieke softwarebedrijf werd gekozen omwille van de lagere loonkosten en het feit dat de algemeen manager een westerse achtergrond had en mogelijke culturele verschillen kan overbruggen. Dit offshoreproject zal overigens uitgebreid worden gevolgd en geëvalueerd om te zien of deze vorm van uitbesteding ook kan worden aangewend voor andere IT-projecten.

Het opzetten van een Y2K-project brengt overigens op een duidelijke manier mogelijke zwakheden van de vigerende IT-praktijken naar boven. De auteur heeft meermalen vastgesteld dat het inventariseren van de gebruikte hardware- en softwareplatformen reeds een pijnlijk probleem was.

*2. Budgettering*
De kosten van een Y2K-inspanning zijn sterk afhankelijk van het aantal en de omvang van programma's, programmaregels en gegevensbestanden die moeten worden omgeschakeld. Een ruwe schatting kan worden gemaakt op basis van de Gartner-cijfers ([Hall96]): 1,10 US dollar per uit-

voerbare LOC (Line Of Code). Voor de berekening worden ook de LOC's geteld die niet moeten worden gewijzigd. De niet-uitvoerbare LOC's daarentegen worden niet meegerekend, wat in het geval van COBOL betekent dat commentaarregels en datadefinities niet worden onderzocht. De schatting bevat alle kosten verbonden aan de verschillende Y2K-fasen: van de strategiefase tot de finale conversie, maar exclusief de kosten van de geautomatiseerde hulpmiddelen, de computertijd, de gebruikersacceptatie, en de algemene aanpassingen inzake standaarden.

Volgens dezelfde bron zal een gemiddeld rekencentrum ongeveer 8000 programma's moeten converteren met elk ongeveer 1500 regels. Indien we ervan uitgaan dat er twintig procent niet-uitvoerbare regels zijn, geeft dit een totale kostprijs van ongeveer 10,5 miljoen US dollar.

De kosten betreffende de expansie van datavelden zijn nog hoger ([Hall96]): 3,00 tot 4,50 US dollar per data-record inclusief de programmawijzigingen. Dit betekent dat een organisatie met zes databases van elk 5 miljoen records, 90 tot 135 miljoen US dollar zal moeten besteden teneinde Y2K-conform te zijn.

In het geval van de Belgische bank werd het aantal te converteren programmaregels geraamd op ongeveer 25 miljoen, wat volgens haar raming resulteerde in een investeringsbedrag van ongeveer 33 miljoen US dollar. Een bijkomend probleem was dat een belangrijk deel van de programma's was geschreven in PL/1, een taal die kostbaarder is om Y2K-conform te maken. COBOL is goedkoper in het detecteren van Y2K-fouten, het verbeteren en het testen ervan. Het merendeel van de conversiesoftware is overigens ontwikkeld voor COBOL, wat logisch is gezien het grote aantal COBOL-applicaties. Dit betekent ook dat COBOL-programmeurs opnieuw veel gevraagd worden en dat sommige opleidingsinstituten opnieuw gestart zijn met het aanbieden van COBOL-cursussen, om in programmeurstekorten te voorzien.

*3. Impactanalyse*
De uitdaging van de impactanalyse bestaat in het gedetailleerd onderzoek van de verschillende source codes met het doel alle datavelden en programma-instructies op te sporen die in aanmerking komen voor wijziging. Deze identificatie kan gebeuren op basis van lijsten met conventies inzake datanamen. Typische datanamen zijn: YYMMDD, DATE, DAT, DT, WS-DATE, CURRENT, EXPIRE, BEGIN, END, TERM, THISDATE, etc. Deze analyse kan handmatig worden uitgevoerd en/of met behulp van geautomatiseerde tools. Voor niet-courante programmeertalen bestaat er meestal geen scanningsoftware en moet de impactanalyse dan ook volledig handmatig worden uitgevoerd.

*4. Ombouwen*
Ombouwen betekent het converteren van de geïnfecteerde programmaregels en -bestanden, en het Y2K-conform maken met interpretatie- en/of expansietechnieken. Dit werk kan gebeuren door gebruik te maken van geautomatiseerde hulpmiddelen. Zoals hiervoor reeds aangegeven, kan deze activiteit worden uitgevoerd door (offshore) outsources; de voorgaande projectactiviteiten worden evenwel bij voorkeur gedaan door eigen mensen of kunnen worden uitbesteed aan consultants.

*5. Conversie en testen*
De testsituatie in een Y2K-project is vrij uniek omdat men niet alleen moet testen of het systeem millennium-conform is, maar ook of het gewijzigde systeem vandaag nog kan werken. Om de situatie 'na 2000' te testen, moet een volledige Y2K-omgeving gecreëerd worden inclusief Y2K-aangepaste versies van hardware en systeemsoftware. Deze testomgeving moet overigens volledig worden gescheiden van het operationele systeem teneinde besmetting te vermijden. Algemeen wordt nu aangenomen dat de testfase meer dan vijftig procent van de projecttijd in beslag neemt. Dit kan zelfs beduidend meer zijn wanneer men te maken heeft met een omgeving die een slecht configuratiemanagement heeft en geen goede testpraktijken heeft geïmplementeerd.

**Y2K- en de euro-conversie**

Een ander aankomend probleem is de introductie van de euro, die de standaardmunteenheid zal worden in januari 1999 en het enige betaalmiddel vanaf het jaar 2002. Dit probleem ontstaat doordat de lokale munteenheden moeten worden omgezet in euro's, doordat ten minste tijdelijk een dubbel valutasysteem zal moeten worden ondersteund, doordat sommige landen opnieuw zullen worden geconfronteerd met decimale waarden en berekeningen en doordat in een oplossing moet worden voorzien voor de afrondingen.

Ondanks het feit dat deze technische zaken vrij dicht liggen bij het Y2K-probleem en dus kunnen worden opgelost met dezelfde geautomatiseerde hulpmiddelen, is de Europese muntharmonisering een meer functioneel thema: commerciële banken bijvoorbeeld zullen euro-conforme systemen ontwikkelen die tevens voorzien in additionele functionaliteiten voor hun klanten. Dit betekent dat de euro-conversie niet alleen een louter technische dimensie heeft maar ook moet worden gezien als een mogelijkheid tot een strategische actie. Van zijn contacten met Belgische financiële instellingen heeft de auteur geleerd dat in de meeste gevallen beide problemen dan ook apart worden behandeld, hoofdzakelijk omwille van de bijkomende functionele eisen.

## COBIT-MODEL

CobiT (Control OBjectives for Information and related Technology) werd recent ontwikkeld als een 'best practices'-standaard inzake het beheer van informatietechnologie ([ISAC96a]). De auteurs van dit beheermodel positioneren het als een brug tussen business *control*-modellen zoals COSO ([COSO94]) en beheermodellen die meer gefocust zijn op informatietechnologieën zoals DTI ([DTI93]).

Het CobiT-model richt zich op specifieke en gede-

**Planning en organisatie**
1. definiëren IT-strategisch plan
2. definiëren informatiearchitectuur
3. bepalen technologische richting
4. definiëren organisatie en verhoudingen
5. beheren investeringen
6. communiceren met management en directie
7. beheren personeel
8. verzekeren conformiteit met externe vereisten
9. schatten risico
10. beheren projecten
11. beheren kwaliteit

**Verwerking en implementatie**
12. identificeren geautomatiseerde oplossingen
13. verwerven & onderhouden applicatiesoftware
14. verwerven & onderhouden technische architectuur
15. ontwikkelen & onderhouden procedures
16. installeren & accepteren systemen
17. beheren wijzigingen

**Aflevering en ondersteuning**
18. definiëren serviceniveaus
19. beheren services door derden
20. beheren performance & capaciteit
21. verzekeren continue service
22. verzekeren systeembeveiliging
23. identificeren & alloceren kosten
24. opleiding geven & trainen gebruikers
25. ondersteunen & adviseren gebruikers
26. beheren van de configuratie
27. beheren van problemen & incidenten
28. beheren gegevens
29. beheren faciliteiten
30. beheren operaties

**Controle**
31. controleren proces
32. verkrijgen onafhankelijke goedkeuring

*Tabel 3. IT-processen ([ISAC96a], vertaald).*

tailleerde beheerdoelstellingen voor 32 IT-processen die geclassificeerd worden in vier domeinen: planning en organisatie, verwerven en implementatie, aflevering en ondersteuning, en controle (zie tabel 3).

### Y2K-CobiT-beheerdoelstellingen

In de context van dit artikel hebben we een duidelijke belangstelling voor de controles van de IT-processen 'verwerven & onderhouden applicatiesoftware' (13), 'verwerven & onderhouden technische architectuur' (14), en 'beheren wijzigingen' (17). Inderdaad, een Y2K-project is een specifiek en uniek onderhoudsproject voor de applicaties en de technische infrastructuur en heeft behoefte aan beheermaatregelen inzake het aanbrengen van wijzigingen (zie tabel 4).

Het zijn algemene beheerdoelstellingen inzake onderhoud en het beheer van wijzigingen die moeten worden toegepast op het Y2K-project. Dit betekent dat een Y2K-project gemakkelijker kan worden gerealiseerd wanneer er reeds goede praktijken inzake onderhoud, management van wijzigingen en configuratiemanagement bestaan. Bij de opstart van een Y2K-project wordt echter dikwijls geconstateerd dat dergelijke procedures en praktijken niet aanwezig zijn en/of niet zijn geïmplementeerd, wat de uitvoering van het Y2K-project sterk bemoeilijkt.

### CobiT-auditrichtlijnen

CobiT ([ISAC96b]) beschrijft de auditrichtlijnen die auditors kunnen gebruiken om de specifieke IT-processen te reviewen en te evalueren ten opzichte van de gespecificeerde beheerdoelstellingen. De waarde van [ISAC96b] ligt hierin dat de opgegeven structuur en elementen bijzonder nuttig zijn bij het opstellen van een auditplan. Deze structuur zal dan ook gevolgd worden in dit artikel. Wij hebben

**Onderhoud applicaties**
- *wijzigingen aan bestaande systemen*: verzekeren dat een gelijksoortig ontwikkelingsproces wordt toegepast als voor de ontwikkeling van nieuwe systemen.

**Onderhoud technische architectuur**
- *preventief onderhoud voor hardware*: IT-management moet periodiek hardwareonderhoud laten uitvoeren.
- *onderhoud systeemsoftware*: procedures moeten worden geïmplementeerd die voorzien in het onderhoud van systeemsoftware.
- *controls inzake wijzigingen systeemsoftware*: procedures moeten worden geïmplementeerd die ervoor zorgen dat de wijzigingen in systeemsoftware worden beheerst en dat dit plaatsvindt volgens de algemene regels inzake het management van wijzigingen.

**Beheer wijzigingen**
- *formele aanvraag voor wijzigingen*: alle aanvragen voor wijzigingen en onderhoud moeten op een geformaliseerde manier gebeuren.
- *impactanalyse*: er moet een procedure zijn die de tijdsduur en kosten inschat van de onderhoudsaanvragen.
- *controle van de wijzigingen*: de controle van het management van de wijzigingen moet geïntegreerd zijn met het configuratiemanagement.
- *vrijgeven van software*: het vrijgeven van software moet formele procedures volgen inclusief de acceptatie door de verschillende partijen.

*Tabel 4. Beheerdoelstellingen voor applicatie-onderhoud, technologieonderhoud, en wijzigingen ([ISAC96a], aangepast).*

*Tabel 5. Auditrichtlijnen voor Y2K-projecten ([ISAC96b], aangepast).*

**1. Verzamelen van basismateriaal:**
- *interviews met:*
  - algemene directie
  - financiële directie
  - IT-directie
  - managers ontwikkeling en operaties
  - systeemanalisten, systeemontwerpers, applicatieprogrammeurs
  - personeel operations
  - projectleider Y2K-project
  - eindgebruikers
  - computer- en softwareleveranciers, outsourcers
- *verzamelen van:*
  - strategisch Y2K-plan
  - Y2K-budgetten en tijdsplanning
  - inventarisatie van applicaties, databases, applicatiepakketten, hardwareplatformen en systeemsoftware
  - benchmarking-rapporten.

**2. Evalueren van de controls:**
- *na te gaan of:*
  - er een plan bestaat dat verzekert dat de organisatie Y2K-conform zal zijn voor het jaar 2000
  - er een inventaris bestaat van hardware en software die Y2K-conform moet worden gemaakt
  - er systemen zijn geïdentificeerd die onvoldoende gedocumenteerd zijn en/of waarvan de source code niet meer beschikbaar is
  - de kwaliteit van de algemene onderhoudsprocedure voldoende is
  - er reeds een nieuwe politiek is ingevoerd die vereist dat alle nieuwe software en hardware millenniumconform is
  - de organisatie de nodige softwareproducten heeft aangekocht voor de detectie, wijziging en testen van de Y2K-problemen
  - management reeds contracten heeft bedongen met consultants en/of (offshore) outsourcers.

**3. Inschatting conformiteit (compliance):**
- *door te testen of:*
  - het Y2K-plan en de inventarisatie volledig zijn
  - de algemene onderhoudsprocedures en -praktijken worden toegepast
  - de algemene testmethoden en -procedures worden toegepast
  - de nieuw aangekochte hardware en software Y2K-gecertificeerd is
  - de algemene bedrijfsregels inzake de selectie van Y2K-geautomatiseerde hulpmiddelen worden gerespecteerd
  - consultants en outsourcers zijn gekozen en gecontracteerd volgens de algemeen geldende bedrijfsregels.

**4. Bevestiging (substantiating):**
- *door het uitvoeren van:*
  - een vergelijking (benchmarking) met gelijksoortige organisaties en/of standaarden
  - een gedetailleerd onderzoek van de Y2K-methodologie met speciale aandacht voor de testfase
  - een gedetailleerde studie van de contracten met leveranciers, consultants en outsourcers teneinde de graad van Y2K-conformiteit te evalueren
- *door het identificeren van:*
  - onvoldoende budgetten, personeel en andere middelen voor de Y2K-conversie
  - ontoereikende of ongeschikte testpraktijken
  - ontoereikende of ongeschikte Y2K-contracten.

tevens gebruikgemaakt van één van de appendices van deze publicatie waarin de CobiT-auditrichtlijnen worden toegepast op het millenniumthema (zie tabel 5).

## CONCLUSIES

Dit artikel bevat een formele audit- en controlbenadering voor een belangrijk computerprobleem dat algemeen bekend is als het Jaar 2000-probleem. De voorgestelde aanpak is gebaseerd op het gestandaardiseerde CobiT-model, aangevuld en gedetailleerd met elementen van Y2K-publicaties die worden geleverd door verschillende Internet-websites.

De meeste op enkele recente seminars over het millenniumfenomeen gepresenteerde praktijkgevallen bevestigen dat het gaat om een zeer risicovol project en dat heel wat ondernemers zich nog niet ten volle bewust zijn van deze problematiek. Een beheerste aanpak zoals beschreven in deze bijdrage is dan ook nodig. Een Y2K-project is geen nachtmerrie of crisissituatie wanneer het wordt aangepakt als een groot en bijzonder onderhoudsproject en de hiervoor geschikte procedures en praktijken worden toegepast:
- opstellen van een strategie en een goed projectplan dat hetzelfde proces volgt als in het geval van een nieuw te ontwikkelen systeem;
- extra aandacht besteden aan de testfase die zeer speciaal is omdat systemen zowel 'voor 2000' als 'na 2000' geschikt moeten zijn;

- toepassen van de algemene bedrijfsregels inzake de aankoop van Y2K-software;
- toepassen van de algemene bedrijfsprocedures inzake leveranciers, consultants en outsourcingpartijen.

## LITERATUUR


[COSO94] COSO, *Internal control – integrated framework*, American Institute of Certified Public Accountants, 1994.

[DTI93] DTI, *A code of practice for information security management*, Department of Trade & Industry, London 1993.

[Eldr96] A. Eldridghe en B. Louton, *A comparison of procedural and data change options for century compliance*, http://www.year2000.com/, 1996.

[Hall96] B. Hall en K. Schick, *Year 2000 crisis: estimating the cost*, Gartner Group, Research note, 1996, KA-210-1262.

[IBM96] IBM, *The year 2000 and 2-digit dates. A guide for planning and implementation*, http://www.software.ibm.com/, 1996.

[ISAC96a] ISACF, *Cobit control objectives*, Information Systems Audit and Control Foundation, Rolling Meadows (Ill.) 1996.

[ISAC96b] ISACF, *Cobit audit guidelines*, Information Systems Audit and Control Foundation, Rolling Meadows, 1996.

[Jage96a] P. de Jager, *Peter de Jager's testimony to House of Representatives. Testimony to Science Committee. Unjustified optimism*, http://www.year2000.com/, 1996.

[Jage96b] P. de Jager, *Systemic triage*, http://www.year2000.com/, 1996.

[Jage97] P. de Jager, *You've got to be kidding*, http://www.year2000.com/, 1997.


*Prof. W. Van Grembergen Is hoogleraar aan de Faculteit Toegepaste Economische Wetenschappen van de UFSIA en aan de UFSIA Management School (IPO). Zijn huidig onderzoek en onderwijs betreft voornamelijk bedrijfstransformaties door middel van informatietechnologie en audit van informatiesystemen. Tot voor kort was hij directeur van het MBA Programma en op dit ogenblik is hij coördinator van een tweejarig IT-auditprogramma.*

# EDP AUDITORIUM

## INFORMATIEBEVEILIGING: HET ONDERGESCHOVEN KIND VAN HET INFORMATICAONDERWIJS

*Ir. ing. P.J. Kleine Punte*

Aan de opleidingsbehoeften op het gebied van informatiebeveiliging wordt bij lange na niet voldaan door het aanbod ervan in opleidingen. Dit blijkt uit een onderzoek dat is uitgevoerd door de twee onderzoekers ir. ing. P.J. Kleine Punte en ir. E.J. Moojen van de Technische Universiteit Eindhoven in opdracht van het Ministerie van Economische Zaken.

De opleidingsbehoeften zijn geïnventariseerd door het verspreiden van vragenlijsten onder de leden van de NGI-afdeling Beveiliging. De organisaties waar deze leden werkzaam zijn, kunnen worden beschouwd voorop te lopen op het gebied van informatiebeveiliging.

Het resultaat van deze inventarisatie van de opleidingsbehoeften op het gebied van informatiebeveiliging is gespiegeld aan het aanbod van 485 relevante opleidingen aan universiteiten, HBO's en niet-reguliere instellingen.

Door de opleidingsbehoeften te vergelijken met het opleidingsaanbod kon worden vastgesteld in welke mate de vraag voldoet aan het aanbod.
Het onderzoek heeft zich echter niet beperkt tot een inventarisatie van vraag en aanbod, tevens is onderzocht welke factoren van invloed zijn op de opleidingsbehoeften.

De geconstateerde opleidingsbehoeften blijken afhankelijk te zijn van een aantal specifieke bedrijfsfactoren.
In de eerste plaats is dat de grootte van de organisatie, weerspiegeld door het aantal medewerkers. Gerelateerd daaraan is het aantal automatiseringsmedewerkers in de organisatie. De opleidingsbehoeften tonen een positieve samenhang met het aantal (automatiserings)medewerkers: hoe meer (automatiserings)medewerkers in een organisatie, des te groter zijn de opleidingsbehoeften. Herkenbare opleidingsbehoeften voor informatiebeveiliging moeten daarom voornamelijk worden gezocht in de grotere organisaties. In kleine organisaties zijn de opleidingsbehoeften voornamelijk latent aanwezig en zullen mogelijk pas in de toekomst manifest worden.

Naast het aantal (automatiserings)medewerkers zijn ook de in de organisatie gehanteerde communicatietechnieken en de wijze van automatisering van invloed op de opleidingsbehoeften. Dit wordt vooral duidelijk bij organisaties die gebruikmaken van EDI, WAN's, mainframes en bij organisaties waarbij de informatievoorziening is geoutsourcd. De complexiteit van de systemen (bijvoorbeeld WAN's) en de mate waarin afspraken moeten worden gemaakt tussen verschillende partijen (EDI en outsourcing) blijken belangrijke oorzaken te zijn voor de behoefte aan opleidingen.

Het feit of in de organisatie een functionaris of afdeling aanwezig is die de verantwoordelijkheid draagt voor de informatiebeveiliging is wellicht de meest saillante factor die invloed heeft op de opleidingsbehoeften. Uit het onderzoek is namelijk gebleken dat in organisaties met een beveiligingsfunctionaris of -afdeling de opleidingsbehoeften zeker twee maal zo hoog zijn als in organisaties zonder een beveiligingsfunctionaris. Dit verschil in opleidingsbehoeften vindt zijn oorsprong in de vraag of er in een organisatie een trekker aanwezig is voor de opleidingsbehoeften op het vlak van informatiebeveiliging. De opleidingsvraag kan in dat geval worden gekoppeld aan een specifieke functionaris of afdeling in de organisatie.

Naast deze bedrijfsgerelateerde factoren bleek ook dat het oordeel over de kwaliteit en over de noodzaak van informatiebeveiliging in de organisatie van invloed is op de opleidingsbehoeften. Is men van oordeel dat de informatiebeveiliging in de organisatie slecht is geregeld, dan bestaan er meer opleidingsbehoeften, wat overeenkomt met de theorieën met betrekking tot opleidingsbehoeften. Hetzelfde geldt voor de mate waarin informatiebeveiliging als noodzakelijk wordt ervaren. Organisaties die informatiebeveiliging minder belangrijk achten, vertonen significant minder opleidingsbehoeften dan organisaties die het wel belangrijk achten.

Met betrekking tot de kwaliteit van de informatiebeveiliging geldt dat de leden van het NGI, afdeling Beveiliging de informatiebeveiliging in hun organisaties gemiddeld genomen als redelijk tot goed beoordelen. Op een aantal terreinen van de informatiebeveiliging worden door de NGI-leden echter nog te veel problemen gesignaleerd. Deze problemen hebben met name betrekking op de naleving van het informatiebeveiligingsbeleid en op risicobeheersing. Op technisch gebied worden relatief weinig problemen gesignaleerd.

## INVENTARISATIE

De opleidingsbehoeften en het opleidingsaanbod zijn geïnventariseerd door middel van een twintigtal kernbegrippen in de informatiebeveiliging, waarbij elk betrekking heeft op een belangrijk aspect van informatiebeveiliging. Voor een overzichtelijke weergave van de opleidingsbehoeften en het opleidingsaanbod worden deze kernbegrippen geclassificeerd in de volgende dimensies: technisch, organisatorisch, bestuurlijk en juridisch. De technische dimensie omvat alle logische en fysieke maat-

regelen. De organisatorische dimensie omvat alle maatregelen die de technische maatregelen ondersteunen en verankeren in de organisatie, zoals bijvoorbeeld procedures en het toewijzen van verantwoordelijkheden. Bestuurlijke aspecten zijn noodzakelijk voor het sturen van het beveiligingsproces en zijn bijvoorbeeld het uitvoeren van een risicoanalyse en het opstellen van een beveiligingsbeleid en -plan. Tot slot zijn er nog juridische randvoorwaarden waarmee rekening moet worden gehouden, zoals bijvoorbeeld de Wet persoonsregistraties en service level agreements die samen de juridische dimensie vormen.

De opleidingsbehoeften en het opleidingsaanbod zullen in het vervolg worden weergegeven in termen van deze technische, organisatorische, bestuurlijke en juridische dimensies.

## OPLEIDINGSBEHOEFTEN EN -AANBOD

Over het algemeen zijn de opleidingsbehoeften op het gebied van informatiebeveiliging met name organisatorisch en bestuurlijk van aard. De belangrijkste kernbegrippen zijn risicoanalyse, risicobeheersing, controle van de informatiebeveiliging, dataclassificatie en het opzetten van een organisatiestructuur voor informatiebeveiliging.

Opleidingsbehoeften zullen echter in het bedrijfsleven afhankelijk zijn van de taken die verschillende functionarissen in de organisatie uitvoeren. In het onderzoek is om deze reden geïnventariseerd hoe de opleidingsbehoeften zijn gedistribueerd over een aantal soorten functionarissen. Enkele van deze functionarissen zijn: informatici, beveiligingsfunctionarissen, EDP-auditors en lijnmanagers. Voor deze functionarissen zullen de opleidingsbehoeften en het opleidingsaanbod hieronder worden weergegeven.

Voor *informatici* wordt in het bedrijfsleven een brede behoefte geconstateerd aan kennis en vaardigheden op het gebied van informatiebeveiliging. Deze behoefte beperkt zich niet uitsluitend tot kennis van technische beveiligingsaspecten, maar betreft ook kennis omtrent het uitvoeren van een risicoanalyse en het ontwerpen van veilige systemen.

De aandacht die in informaticaopleidingen wordt besteed aan informatiebeveiliging is zeer gefragmenteerd en beperkt zich doorgaans tot cryptografie en een enkel keuzevak met betrekking tot informatiebeveiliging.

Het beperkte aanbod in opleidingen heeft tot gevolg dat de gemiddelde informaticus na zijn opleiding niet voldoende bekend is met het begrip informatiebeveiliging, en niet of nauwelijks in staat is een betrouwbare informatievoorziening te waarborgen of betrouwbare en veilige informatiesystemen te ontwikkelen of te onderhouden.

Ook voor *beveiligingsfunctionarissen* wordt een grote opleidingsbehoefte geconstateerd. De beveiligingsfunctionaris moet niet alleen een grondige technische kennis bezitten van informatiebeveiliging, maar ook een uitgebreide kennis van organisatorische en bestuurlijke maatregelen op beveiligingsgebied. Tegenover de opleidingsbehoeften die zijn gesignaleerd voor informatiebeveiligingsfunctionarissen staat echter nauwelijks enig aanbod in opleidingen.

Deze conclusies staan in sterk contrast met het niveau dat inmiddels voor EDP-auditing is bereikt. Volgens het onderzoek is er ruim voldoende aandacht voor het *controleren* van informatiebeveiligingsmaatregelen, in de vorm van EDP-auditopleidingen en -modulen. Er is echter spaarzaam aandacht voor het *implementeren en sturen* van deze maatregelen.

Dat de opleidingen voor EDP-auditors van een hoog niveau worden gevonden, mag slechts een schrale troost heten. Het niveau van EDP-auditopleidingen zou als voorbeeld moeten dienen voor opleidingen voor beveiligingsfunctionarissen, iets waaraan een duidelijke behoefte bestaat. Het accent in de opleiding dient hierbij verschoven te worden van controleren van de informatiebeveiliging naar de implementatie ervan.

Tot slot zijn ook voor het *lijnmanagement* opleidingsbehoeften gesignaleerd. Gezien de taken die lijnmanagers vervullen in de organisatie, zijn de opleidingsbehoeften van een andere aard dan voor de andere beschreven functionarissen. Terwijl het lijnmanagement minder kennis hoeft te bezitten van technische aspecten van de beveiliging, ligt de nadruk meer op organisatorische en bestuurlijke kennis en vaardigheden, waarmee het proces van informatiebeveiliging gestuurd en gecoördineerd kan worden. Informatiebeveiliging betekent voor de lijnmanager voornamelijk het zorg dragen voor risicobeheersing en kwaliteitszorg. Van het opleidingsaanbod voor lijnmanagers - dat voornamelijk moet worden verzorgd door niet-reguliere instellingen - is vastgesteld dat de kwaliteit sterk varieert en dat het aanbod als onoverzichtelijk wordt bestempeld.

## AANBEVELINGEN

Voor informatiebeveiliging is het gebrek aan *bewustzijn* een bekend probleem, dat ook in het bedrijfsleven wordt ervaren. Dit kan de implementatie van informatiebeveiliging belemmeren. Om het bewustzijn te verbeteren wordt in het onderzoek een aantal instrumenten aanbevolen, zoals het gestructureerd aandacht besteden aan basiskennis en vaardigheden met betrekking tot informatiebeveiliging, te beginnen in het voortgezet onderwijs, en door het verstrekken van voorlichtingsmateriaal.

Voor het *management* wordt aanbevolen aan te haken bij reeds lopende activiteiten, zoals in het kader van kwaliteitszorg, beheer van de IT-infrastructuur of de permanente educatie.

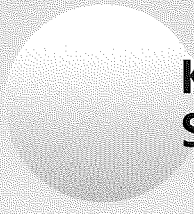
Om het aanbod aan opleidingen voor *informatici* te verbeteren wordt aanbevolen in informaticaoplei-

dingen enkele modules of specialisaties op te nemen waarin de informatiebeveiliging centraal staat. De volgende titels worden daarbij voorgesteld: 'Kwaliteit van de informatievoorziening' en 'Betrouwbare telecommunicatieoverdracht'.

Een derde aanbeveling is gericht op de behoefte aan *beveiligingsfunctionarissen* die hun technische inzicht kunnen combineren met bestuurlijke en organisatorische vaardigheden. Een opzet in die richting kan worden bereikt door een specialisatie gericht op het kunnen managen van informatie en de daaraan verbonden risico's. Daarbij moeten de organisatie, haar wensen en de informatiestromen centraal staan.

Om deze aanbevelingen vorm te geven is het vooral van belang dat bedrijfsleven en onderwijsinstellingen veelvuldig en intensief met elkaar van gedachten wisselen over de gewenste vorm en inhoud van het informaticaonderwijs in het algemeen en opleidingen op het gebied van informatiebeveiliging in het bijzonder.

*Het rapport 'Informatiebeveiliging: Opleidingsbehoeften van organisaties en het aanbod in Opleidingen' is kosteloos te verkrijgen bij het Ministerie van Economische Zaken (tel. 070-3798820). Voor vragen over het onderzoek kunt u zich wenden tot ir. ing. P.J. Kleine Punte (tel. 020-4001172).*



KPMG EDP Auditors
Samsom BedrijfsInformatie