EDP-auditing in relatie tot management

Het exclusiviteitsvraagstuk

Mw. Prof. M. E. van Biene-Hershey

1 Inleiding

In de oratie 'EDP-Auditing in relatie tot Management'[1] wordt het onderwerp exclusiviteit behandeld. Tijdens het uitspreken van de inaugurele rede op 20 januari 1989 aan de Vrije Universiteit bestond onvoldoende gelegenheid nader op het exclusiviteitsvraagstuk in te gaan.
Mede gezien de actualiteit van dit onderwerp in het kader van de privacywetgeving zullen in het onderhavige artikel in bijzonder de systemen en controlemaatregelen ter zake behandeld worden. Deze systemen en controlemaatregelen zijn voor een edp-auditor van essentieel belang als hij, voortvloeiend uit de privacywetgeving of in het kader van een ruimere managementopdracht, een beoordeling van de exclusiviteit gaat uitvoeren.
Tenslotte zal het privacywetsvoorstel van enkele kritische kanttekeningen worden voorzien.

In de oratie en ook in dit artikel wordt nadrukkelijk afstand genomen van de edp-audit in het kader van de accountantscontrole en de 'financial audit'. Centraal staan de diepgang en de draagwijdte van edp-auditing met het management als opdrachtgever.
Binnen het huidige begrippenkader van auditors is het onderscheid tussen maatregelen van interne controle en aspecten van de audit – of zo u wilt controledoelstellingen – niet scherp genoeg afgebakend.
Auditaspecten – of zo u wilt controledoelstellingen – zijn kwaliteiten waarvoor in de organisatie en/of bij de auditor normstellingen bestaan en ten aanzien waarvan de auditor zijn onpartijdig oordeel uitspreekt. Interne controle wordt gebruikt in de betekenis van het Engelse woord 'control', dus in de betekenis van beheersing.[2]
In iedere organisatie, die onderworpen wordt aan een audit, bestaat een relatie tussen de interne controlemaatregelen en de auditaspecten. De matrix in figuur 1 laat zien dat er geen één op één relatie is tussen interne controlemaatregelen en auditaspecten. De samenhang zal bovendien verschillen van organisatie tot organisatie.
Een belangrijk deel van de werkzaamheden van de auditor is het bepalen van de toereikendheid van de totale samenhang van interne controlemaatregelen in relatie tot de specifieke auditopdracht.[3]

2 Het exclusiviteitsvraagstuk

Dit artikel heeft tot doel een beeld te geven van de vele facetten van de realisatie van een edp-audit opdracht. De beschouwde opdracht betreft het beoordelen van de sterktes en zwaktes in de organisatie met betrekking tot het exclusiviteitsvraagstuk. Praktische aandachtsgebieden ten behoeve van een dergelijke opdracht krijgen de nadruk.
Edp-auditing is de functie die onder andere namens de niet ter zake deskundigen beoordeelt of de vereiste waarborgen in automatisering worden gerealiseerd zodat met name het geheel effectief is. Slechts met een beheersbare automatisering kan onze samenleving zich op verantwoorde wijze ontwikkelen. Een adequate invulling van het exclusiviteitsvraagstuk is een voorwaarde voor deze harmonieuze ontwikkeling. Een bijzon-

Mw. M. E. van Biene-Hershey is hoogleraar edp-auditing aan de Vrije Universiteit en onderdirecteur bij de Amrobank.

dere verschijningsvorm van het exclusiviteitsvraagstuk is het privacyvraagstuk.
De commissie-Franken heeft het begrip exclusiviteit geïntroduceerd.[4]
De volgende definitie wordt van de door de commissie gegeven omschrijving afgeleid:

> een toestand waarin activa uitsluitend worden gebruikt door daartoe bevoegde personen conform goedgekeurde procedures.

Het belang van toereikende maatregelen ter waarborging van de exclusiviteit is duidelijk, het individu en de maatschappij zijn erbij gebaat. Maatregelen van autorisatie, access control en authenticatie dragen in belangrijke mate bij tot een adequate invulling van de exclusiviteit.
De hiervoor genoemde categorieën van maatregelen kunnen als volgt nader worden omschreven:
- autorisatie is de delegatie van bevoegdheden;[5]
- bevoegd gebruik houdt in de middelen die waarborgen dat de autorisatieregels niet worden geschonden;
- authenticatie is het waarborgen van een juiste identificatie van instanties die toegang tot resources wensen.

De beschouwing van deze maatregelen beperkt zich tot die maatregelen die gerangschikt kunnen worden onder 'general controls'. Dit zijn beheersingsmaatregelen met betrekking tot de algehele interne organisatie met het doel te verzekeren dat de ontwikkeling, implementatie en operations van de organisatie op een ordelijke wijze plaatsvindt. Deze maatregelen bevinden zich in het bijzonder in een aantal gemeenschappelijk gebruikte systemen van de geautomatiseerde organisatie. Bijvoorbeeld in het databasemanagementsysteem, het besturingssysteem, de datacommunicatiesoftware en de hardware. Als zodanig vereisen zij de aandacht van de edp-auditor wanneer het exclusiviteitsvraagstuk wordt beoordeeld. De maatregelen ter realisatie van een toereikend niveau van exclusiviteit worden derhalve voornamelijk opgenomen in:
- de datacommunicatie infrastructuur;
- de implementatie van het besturingssysteem;
- de databasemanagementsystemen; en
- de daarmee samenhangende interne organisatie.

2.1 Autorisatie
Om bevoegdheden te kunnen delegeren moet er sprake zijn van een verantwoordelijkheidstelling. Helaas is het in een modern geautomatiseerd bedrijf geen eenvoudige taak om vast te stellen wie voor wat verantwoordelijk is. Met name de tendentie naar non-redundante bestanden en geïntegreerde processen heeft het vaststellen van de gebruikersverantwoordelijkheden steeds moeilijker gemaakt.
Wanneer de structuur van de administratieve automatisering niet aansluit op de verantwoordelijkheidstellingen in het bedrijf, ontstaat er een groot probleem bij de delegatie van bevoegdheden voor raadplegen en muteren. Met name is dit het geval bij delegaties die plaatsvinden in een organisatie waarin de computer werkelijk de spil van de bedrijfsuitoefening is.
Het oplossen van deze delegatieproblemen geschiedt veelal door het instellen van de functie van informatiemanager. Deze informatiemanager is dan vervangend voor de lijnmanager en hij moet ervoor zorgen dat de lijnmanager een effectieve automatiseringsondersteuning ondervindt. De informatiemanager wordt geacht zowel de beleidsmatige problemen ten aanzien van de informatievoorziening, als de operationele delegatieproblemen op te lossen.
Een voor een ieder duidelijke delegatie van bevoegdheden is de basis voor de inrichting van de maatregelen die het bevoegd gebruik van automatiseringsmiddelen regelen.

Naast het expliciet maken van verschillende verantwoordelijkheden is het ook nodig dat het management mensen, informatie en automatiseringsmiddelen indeelt in een beveiligingsclassificatiesysteem. Dit is nodig om onderscheid te kunnen maken in risicogevoeligheid, zodat de noodzakelijke maatregelen per klasse kunnen worden getroffen. Wanneer deze activiteit is verricht, kan worden overgegaan tot het implementeren van de maatregelen in de automatiseringsomgeving.
De belangrijkste geautomatiseerde interne con-

trolemaatregelen ter ondersteuning van de exclusiviteit betreffen het bevoegd gebruik van automatiseringsmiddelen.

2.2 Bevoegd gebruik

Als eerste wordt een behandeling van dit onderwerp in relatie tot het databasemanagementsysteem gegeven. Immers het database managementsysteem regelt de toegang tot data in de database. Veel hiërarchische databasemanagementsystemen verschaffen in samenhang met een goede databasestructuur een goed niveau van bevoegd gebruik.[6] Een beoordeling van de maatregelen getroffen in het databasemanagementsysteem en in de databasestructuur is vereist. Maar het management moet expliciet maken wie, wat en wanneer mag. Pas op, het 'wanneer' wordt bij mijn weten niet door het databasemanagementsysteem opgelost. Dus blijft over wie mag wat.

Het besturingssysteem kan de beschikking hebben over een verbijzonderd 'access control mechanism' (n.b. access control is de Engelse term voor bevoegd gebruik). Deze pakketten kunnen soms de 'wanneer' vraag voor u regelen.

Het Amerikaanse Ministerie van Defensie heeft een classificatiesysteem ontworpen voor de indeling van de overall beveiligingsstructuur van besturingssystemen.[7] Op één na waren alle commercieel gebruikte besturingssystemen in 1986 geclassificeerd als C2 of lager.[8] A en B zijn classificaties voor de beter beveiligde systemen en D is de laagste classificatie. Voorwaarde voor het verkrijgen van een niveau B classificatie is dat het bevoegd gebruik mechanisme geen verbijzonderde interne controle is (een gespecialiseerd pakket) maar een geïntegreerd onderdeel vormt van de structuur van het besturingssysteem. Verbijzonderde interne controle wordt derhalve minder sterk geacht dan in de lijn geïntegreerde controle.

Een besturingssysteem heeft altijd enigerlei vorm van access control nodig omdat een besturingssysteem zelf bijna niets anders doet dan het regelen van het gebruik van resources. Dit betreft echter een ander niveau dan de bewaking van het juiste gebruik van gegevens zoals dat uitgevoerd wordt door een databasemanagementsysteem. Het access control mechanisme in het besturingssysteem moet men beoordelen.

Een datacommunicatieverbinding maakt het mogelijk dat een gebruiker op afstand een computerinstallatie kan benutten. Een besturingssysteem heeft de plicht ook het gebruik van computerresources door middel van datacommunicatie op rechtmatigheid te controleren.

De vraag is of het effectief is, dat de datacommunicatie infrastructuur in principe alles zonder discriminatie doorstuurt naar een besturingssysteem voor de controle op bevoegd gebruik. Velen vinden dit acceptabel. Ze stellen dat de zogenaamde 'end to end control' – buiten de datacommunicatie infrastructuur om – de meest effectieve oplossing is.

Er zijn echter twee redenen om het hiermee oneens te zijn:

- efficiëntie overwegingen zowel betreffende het datacommunicatienetwerk als met betrekking tot de centrale computersystemen;
- het huidige niveau van beveiliging van besturingssystemen en computerinstallaties in het algemeen.

Voor wat dit tweede punt betreft, wordt verwezen naar de standaarden van het Amerikaanse Ministerie van Defensie en naar de literatuur over de structurele tekortkomingen in de beveiligingsarchitecturen van de grote mainframes. Ten aanzien van de efficiëntie zijn enkele opmerkingen over datacommunicatienetwerken op zijn plaats.

Het afstemmen van de infrastructuur op de bevoegdheden voor gebruik van een datacommunicatienetwerk betekent simpelweg dat onbevoegden geen gebruik kunnen maken van de, altijd beperkt beschikbare capaciteiten.

De noodzaak om maatregelen in de datacommunicatie infrastructuur te treffen, die het onbevoegd gebruiken van datacommunicatiemiddelen voorkomen, wordt nu algemeen geaccepteerd.[9] Hierdoor is de ontwikkeling van de noodzakelijke faciliteiten gestimuleerd. Tegenwoordig bestaat er een groot aantal technische oplossingen.

De beoordeling van de structuur van het datacommunicatienetwerk en de in het netwerk

getroffen maatregelen van bevoegd gebruik is vereist. Een voorwaarde voor de realisatie van een effectief bevoegd gebruik is het vaststellen van de juiste oorsprong van de gegevens. Dit hangt nauw samen met de nu te behandelen laatste categorie van maatregelen in het kader van de exclusiviteit, namelijk, de authenticiteit.

2.3 Authenticiteit

Het vraagstuk van de authenticiteit is eenvoudig uit te leggen. Alles in de computer en in de datacommunicatieverbinding wordt gereduceerd tot nullen en enen. Als men in staat is om de specifieke voorstelling van nullen en enen die uw buurman toegang geeft tot een computerinstallatie in te toetsen op het eindstation, dan is men in staat, voor wat de computer betreft, zich voor te doen als de buurman. De computer zal dan even behulpzaam zijn alsof u uw buurman was. In een geautomatiseerde omgeving zijn ook voor een ieder bekende namen nodig. Hiervoor gelden dezelfde redenen als voor de bekendheid van een telefoonnummer.

Een algemene naam is echter niet toereikend voor authenticatiedoeleinden. Dit vereist de toepassing van zogenaamde authenticatiemiddelen waarmee vastgesteld kan worden dat men werkelijk degene is wie men zegt te zijn. Deze extra identificatiehandeling dient gebaseerd te zijn op een handeling die alleen door één persoon kan worden uitgevoerd. Dit is de zogenaamde authenticiteitsslag. Er zijn vele authenticiteitsmiddelen.[10]

Authenticiteitsmiddelen hebben in een moderne automatiseringsomgeving meer functies dan alleen de vaststelling dat je bent wie je zegt dat je bent. Het is bijvoorbeeld in vele bedrijfsprocessen noodzakelijk achteraf vast te stellen wie verantwoordelijk is geweest voor een bepaalde computermatige handeling. Het op deze wijze afleggen van verantwoording vereist toereikende authenticatiemiddelen.

Explicieter geformuleerd, als de totaliteit van de interne controlemaatregelen geen toereikende waarborgen geeft voor een verantwoordelijkheidstelling achteraf, dan dient in die gevallen waarbij de verantwoordelijkheidstelling een vereiste is te worden afgezien van geautomatiseerde ondersteuning.

De commissie-Franken heeft veel werk gemaakt van het vraagstuk van computerfraude en de noodzaak tot wetgeving die vervolging van fraudes mogelijk maakt. Maar als de systemen niet zodanig gebouwd worden, dat de verantwoordelijkheden op een doeltreffende manier kunnen worden gedelegeerd en tijdig controle kan plaatsvinden, zouden deze systemen nooit operationeel mogen worden. Het operationeel maken van zulke inadequate systemen is op zichzelf een onaanvaardbare beslissing. Een wetgeving die hiermede rekening houdt, kan een hoger beschermingsniveau afdwingen, mits de middelen beschikbaar zijn om het hogere beschermingsniveau te bereiken.[11]

3 De privacywetgeving

3.1 Door de wet gestelde eisen

In welke mate de geautomatiseerde administratieve organisatie van een bedrijf voldoet aan de door de Wet persoonsregistraties gestelde eisen is een vraag die vele managers zich zullen stellen. Het eerste deel van de wet is op 1 juli 1989 in werking getreden. Hierdoor is deze vraag zeer actueel geworden.

Er is veel discussie over de interpretatie van de wet met betrekking tot de draagwijdte van de wetgeving bij geautomatiseerde persoonsregistraties.

Van belang hierbij is tevens de discussie over het begrip 'persoonsgericht', zoals gebruikt in het vergaderstuk 19 090 nr. 9 van het vergaderjaar 1986-1987 van de Tweede Kamer. Op pagina 1 wordt het begrip persoonsgericht geïntroduceerd als nadere afbakening van de aard van gegevens in een tekstverwerkende omgeving die al of niet onder de Wet persoonsregistraties vallen.

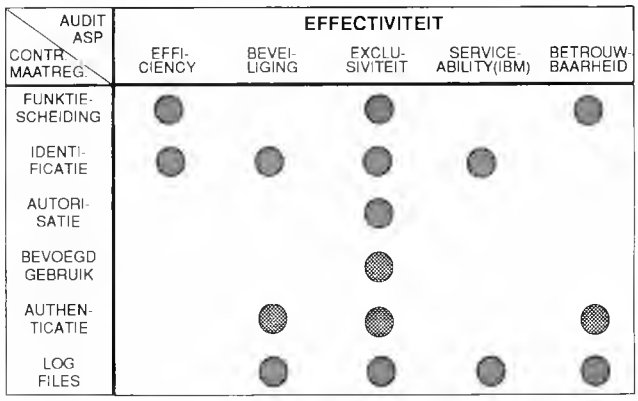
In dit hoofdstuk wordt getracht vanuit de Wet persoonsregistraties een gefundeerd antwoord te geven op de volgende vraag:

Zijn alle gegevens die technisch gezien tot een persoon herleidbaar zijn per definitie persoonsgegevens?

Het antwoord hierop is:
Slechts persoonsregistraties met het doel een persoon te omschrijven en te administreren vallen onder de Wet persoonsregistraties. Vanzelfsprekend zal de wet van toepassing zijn op iedere registratie waarin persoonsgerichte gegevens worden geadministreerd.

Omgekeerd wanneer de registratie niet tot doel heeft een persoonsregistratie te zijn en er worden geen persoonsgerichte gegevens in de registratie bijgehouden en de registratie is geen onderdeel van een persoonsregistratie is de registratie geen persoonsregistratie.
Bij het lezen van de wet en de Memorie van Toelichting is het van belang te onderkennen dat internationale standaardterminologieën met betrekking tot informatie- en dataverzamelingen niet worden gebruikt. Mijn specifieke kritiek richt zich op het verzuim van de wetgever om de relatie tussen de wet en het – als standaard erkende – ANSI-SPARC model duidelijk te maken[12] (zie figuur 2). Dit maakt het zeer moeilijk voor de automatiseerder en edp-auditor om te weten hoe de automatiseringsomgevingen moeten worden ingericht respectievelijk moeten worden beoordeeld, zodat zij adequaat zijn.
Door het taalgebruik te beperken tot terminologieën uit de 'real world' lijkt het alsof de wet slechts tot doel heeft de omgang met een bepaalde soort informatie in de 'real world' te reglementeren. Dit is echter een onjuiste voorstelling. Er wordt verwacht dat de wetgeving gevolgen heeft voor structuur en bestanden, aard van verwerkingsprocessen en maatregelen van verantwoordelijkheidstellingen in de organisatie.
Het proces van deductie van de 'real world' begrippen naar de geautomatiseerde vastleggingen en omgekeerd, is niet omschreven. Dit heeft tot gevolg dat woorden zoals persoonsregistratie en persoonsgegevens zweven tussen de real world en de data processing.
De wet is echter duidelijk in haar intenties (paragraaf 2 van de Memorie van Toelichting):
a ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens;
b inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt alsmede op verbetering van zodanige gegevens.

Figuur 1: Voorbeelden van de relaties tussen maatregelen van control en audit aspecten



Voor een samenvatting van de belangrijkste wetteksten waarop de volgende interpretatie betrekking heeft wordt verwezen naar bijlage 4 van noot 1.

3.2 Uitgangspunten en interpretaties
1 Er is geen één op één afbeelding van het begrip persoonsregistratie en een intern model (fysiek te onderscheiden verzameling data).
2 Informatie is een proces dat plaatsvindt ten aanzien van data. Een persoonsregistratie in de zin van de wet is een afbakening van een deelverzameling uit een conceptueel model. Dus is het begrip persoonsregistratie in de zin van de wet een extern model. Derhalve is het begrip 'koppelen' niet meer relevant in de wetgeving. Het doel van de persoonsregistratie wordt met name bepaald door de processen die men uitvoert ten aanzien van de gegevens (data): de informatieverstrekking. Voor de wet is de bepalende factor de doelstelling van de persoonsregistratie.
3 Een relatie gelegd binnen het interne model heeft alleen waarde in de real world wanneer:
a er programma's zijn die gebruik maken van de relatie;
b de relatie systematisch wordt onderhouden door expliciete administratieve processen en/

of regels waarmede de integriteit van de relaties en de betrouwbaarheid van de procedures controleerbaar is. Anders kan er geen sprake zijn van een door de organisatie bewust aangelegde relatie met als doel aan een bepaalde informatiebehoefte te voldoen.

Er is slechts sprake van een systematisch toegankelijke registratie in de geautomatiseerde omgeving wanneer aan beide criteria (a en b) wordt voldaan. Dit betekent dat ondanks een gelijk gedefinieerd data-item in twee verschillende delen van het interne model, waarbij er administratief-organisatorisch gesproken geen waarborgen zijn voor de consistentie van waarden van het data-item en er ook geen programma's in het bedrijf bestaan voor het gebruik van deze twee delen van het intern model, geen sprake is van een systematisch toegankelijke registratie in de zin van de wet. De theoretische 'informatie' kan niet worden geleverd. Er bestaan namelijk geen programma's die die informatie leveren; er is administratief-organisatorisch geen basis om de juistheid van het gebruik van een dergelijke 'toevalligheid' te garanderen en dus is 'informatie' op basis hiervan mogelijkerwijs desinformatie.

4 De door het bedrijf expliciet gemaakte doelstelling van het gebruik van de persoonsregistratie betekent een beperking van de vrijheid van het bedrijf om:

- persoonsgerichte informatie te verschaffen aan externe instanties zonder toestemming van de persoon in kwestie;
- buiten de door de wet omschreven kaders, programma's te schrijven die informatie kunnen leveren die buiten de doelstelling van de persoonsregistraties zouden vallen.

In formele zin betekent dit dat het bedrijf dan ook geen entiteiten mag toevoegen aan het conceptuele model die niet reeds voorzien zijn in de doelstelling van het gebruik van persoonsregistraties. Dit betekent procedures en automatiseringstechnische maatregelen ter voorkoming van schendingen van de Wet persoonsregistraties.

5 Het is niet de bedoeling van de wet dat geregistreerden door middel van inzagerecht informatieverstrekkingen kunnen verlangen van gegevens die het betreffende bedrijf niet onderhoudt.

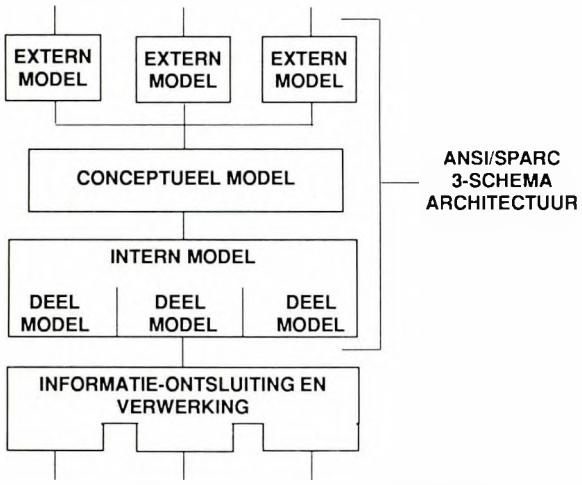
6 De interpretatie van het begrip gegevens, zoals gebruikt in paragraaf 7[13] van de Memorie van Toelichting 'Voor een burger is het van belang te weten welke gegevens over hem in een persoonsregistratie zijn opgenomen en welk gebruik daarvan wordt gemaakt' is: Gegeven een persoonsregistratie waarvan de doelstelling enzovoort is vastgelegd conform de wetgeving, bestaat een al of niet expliciete transformatie van deze omschrijving naar een extern model en daarvan noodzakelijkerwijs naar een conceptueel model en van een conceptueel model naar een intern model. Vervolgens zijn er programma's beschikbaar die uitsluitend conform hetgeen in de doelstelling van de registratie beschreven is functioneren. Omdat het bedrijf een limitatieve opstelling heeft gepubliceerd van de persoonsregistraties en de doelstellingen is het mogelijk voor de burger om volledig inzicht te verkrijgen in de inhoud van de persoonsgerichte data-items = gegevens die betrekking hebben op zijn persoon (de waarden van data-items voor zover de waarden betrekking hebben op zijn persoon). Wanneer dit reductieproces niet opgaat moet geconcludeerd worden dat de omschrijving van de persoonsregistratie in de zin van de wetgeving onjuist of inadequaat is.

4 Samenvatting en conclusie

De eis van exclusiviteit speelt een vooraanstaande rol bij edp-auditing. Dit geldt zowel voor een edp-audit opdracht uitgevoerd in het kader van de privacywetgeving als een algemene edp-audit ten behoeve van het management. De geautomatiseerde administratieve organisatie is niet effectief als niet voldaan wordt aan deze noodzakelijke voorwaarde.

Bij de implementatie van exclusiviteit zullen de controlemaatregelen; autorisatie, bevoegd gebruik en authenticatie gehanteerd moeten worden. De middelen teneinde in die controlemaatregelen te voorzien hebben verschijningsvormen op verschillende niveaus. Derhalve dient een afweging plaats te vinden hoe deze maatregelen worden opgenomen in de datacommunicatie

Figuur 2: Conceptueel schema voor gegevensrepresentatie



DEFINITIES VAN CONCEPTEN IN HET ANSI/SPARC MODEL

extern model:
Dit is de weergave van de informatiebehoefte voor een specifieke toepassing. Het beschrijft slechts een deel van de totale verzameling concerngegevens. Elk extern model is toegespitst op een bepaalde toepassing.

intern model:
Dit deel beschrijft de totale verzameling concerngegevens in implementatietermen.

conceptueel model:
Dit model beschrijft het model van alle objectsystemen die in het intern model moeten worden afgebeeld. Het model bevat beschrijvingen van alle specifieke informatiebehoeften (externe modellen).

infrastructuur, het besturingssysteem, het database managementsysteem en/of de interne organisatie.

De privacywetgeving vereist controle op naleving. Niet alleen vanuit het management bezien maar met name ook ter bescherming van het individu. Het niet gebruiken van standaardterminologieën en het niet onderkennen van de conceptuele niveaus in de gehanteerde definities zal de naleving en de toetsing op naleving van de wet niet vereenvoudigen. Een goed opgeleide edp-auditor zal hieraan een belangrijke bijdrage moeten leveren.

Noten

1 M. E. van Biene-Hershey, *Edp-auditing in relatie tot management,* Vrije Universiteit, Amsterdam, januari 1989.
2 R. W. Starreveld, *Bestuurlijke informatie verzorging deel I: algemene grondslagen,* Samsom, Alphen aan den Rijn, 1981.
3 Systems Auditability & Control Study, The Institute of Internal Auditors, Inc., Altamonte Springs, Florida 1977.
4 Informatietechniek & Strafrecht, Rapport van de Commissie Computer-Criminaliteit, Staatsuitgeverij, Minister van Justitie, 1987.
5 H. Roos, R.A., et.al., *Database en accountant,* Samsom, 1977.
6 E. B. Fernandiz. et.al., *Data base Security and Integrity,* Addison Wesley Publishing Company, Inc., Philippines, 1981.
7 Department of Defense Trusted Computer System Evaluation Criteria, Fort George G. Meade, Maryland 20755, 1983.
8 T. A. Parker, 'The Implementation of a Mandatory Security Policy in a Mainframe Operating System', Conference Proceedings of the Second European Conference on Computer Audit, Control & Security, NGI/EDPAA, 1987.
9 I. J. Douglas, P. J. Olson, *Audit and Control of Computer Networks,* NCC Publications, 1986.
10 Michael B. Wood, *Computer Access Control,* NCC Publications, Manchester, 1985.
11 The Security of Network Systems, a Study on Behalf of the Commission of European Communities, Coopers & Lybrand, 1988.
12 F. R. McFadden, J. A. Hoffer, *Data Base Management,* The Benjamin/Cummings Publishing Company, California, 1985.
13 Memorie van Toelichting op het wetsontwerp Wet persoonsregistratie, Kamerstuk 19 095 3.