KWARTAALBLAD EDP-AUDITING

# 1992/3

ELECTRONIC DATA INTERCHANGE

# COMPACT HERFST

**Compact ®**
*Jaargang 19, nummer 3*
*Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.*
*Het blad verschijnt 4 x per jaar.*

**Redactie**
*D. Steeman RA (hoofdredacteur)*
*drs. R.G.A. Fijneman RE RA*
*prof. A.W. Neisingh RE RA*
*drs. P. Veltman RE RA*

**Redactiesecretariaat**
*Mw. A.M.F. Hofland*
*KPMG Klynveld EDP Auditors*
*K.P. van der Mandelelaan 41*
*3062 MB Rotterdam*
*Tel.: 010 - 453 47 40*
*Fax : 010 - 453 47 77*

**Vormgeving**
*Bureau Karakter, Delft*

**Aan dit nummer werkten mee**
*P. van Berge /*
*drs. M.A. Bongers RE /*
*G.J. Endenburg RI / J.W.J. Laan /drs. G.C.M. Mol /*
*mw. drs. M. Steeman /*
*drs. J.F.H. Vrins*

**Abonnementen**
*f 135,- per jaar incl. BTW. Losse nummers f 45,- 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.: 01720 - 6 68 00*
*Fax : 01720 - 7 59 33*
*Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.*



**Uitgever**
*J.R.M. Masselink*

*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 automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacy-wetgeving • computercriminaliteit en nieuwe regelgeving. Behalve voor EDP-auditors kan dit blad ook interessant zijn voor EDP-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG Klynveld EDP Auditors.*

*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 Klynveld, KPMG Klynveld 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.*

In de herfstuitgave van Compact speciale aandacht voor het fenomeen Electronic Data Interchange, beter bekend als EDI. Nu de invoering van EDI in de praktijk meer en meer gestalte krijgt, is aandacht voor dit onderwerp vanuit het gezichtspunt van de EDP-auditor te rechtvaardigen. Wellicht doordat EDI een overwegend "technology pushed" ontwikkeling is, lijkt in de praktijk aan de (technische) werking van op EDI gerichte toepassingen meer aandacht te worden besteed dan aan de beheersing ervan.

Reeds vele publikaties zijn verschenen met betrekking tot dit onderwerp. Teneinde niet te vervallen in opnieuw een theoretisch betoog over EDI is een aantal direct bij EDI-toepassingen betrokken personen gevraagd een beschouwing te geven van de praktische gevolgen van het gebruik van EDI in hun organisatie. Het resultaat hiervan is een drietal artikelen, waarin onder meer wordt ingegaan op de gevolgen van het gebruik alsmede de beheersing van EDI in de praktijk. Het feit dat elke auteur werkzaam is bij een organisatie in een andere sector (financieel, logistiek en overheid) zorgt ervoor dat telkens andere aspecten van het gebruik van EDI zijn belicht.

Naast voornoemde praktische beschouwingen is in deze uitgave toch ook een artikel over EDI met een wat meer theoretische invalshoek opgenomen. Vooruitlopend op het winternummer met als thema elektronisch bankieren besteedt deze Compact aandacht aan de terughoudendheid van de banken met betrekking tot EDI. Omdat de financiële afhandeling van transacties in elke branche een centrale rol speelt is deze beschouwing zeker niet alleen interessant voor lezers werkzaam in het bankwezen.

Tot slot in deze uitgave aandacht voor de beheersing van het gebruik van informatietechnologie (IT). Min of meer aansluitend op het thema van de vorige Compact - bedrijfseconomische aspecten van IT - wordt een praktische aanpak gepresenteerd voor het opzetten van een beheersstructuur rondom het gebruik van IT. Daar ook EDI kan worden gezien als een toepassing van IT, sluit dit artikel praktisch naadloos aan op de voorafgaande artikelen.

Ondanks of misschien juist dankzij het thema een gevarieerd nummer, waarmee wij de lezers van nuttige informatie denken te voorzien.

M. Groesz

# De EDI-infrastructuur bij de Kas-Associatie

P. van Berge

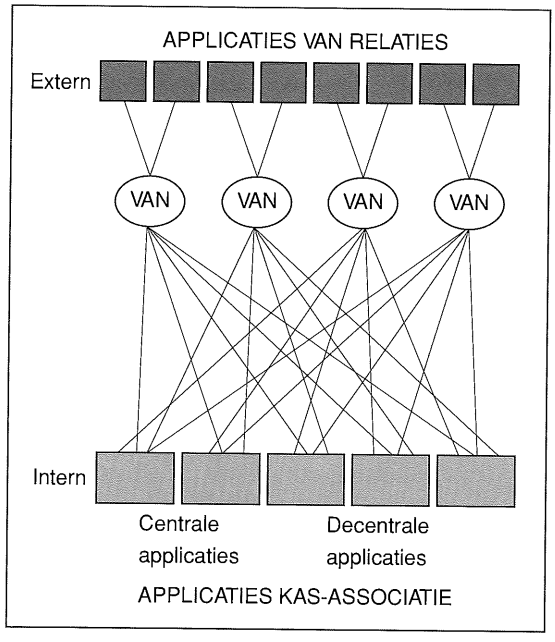
**De voordelen van het toepassen van EDI zijn bekend, de technologische mogelijkheden aanwezig. Is dit voldoende basis voor het invoeren van elektronisch berichtenverkeer of dienen vooraf de gevolgen voor de beheersing te worden geïnventariseerd? Van Berge geeft aan op welke wijze binnen de Kas-Associatie aandacht is geschonken aan de interne controle en beveiliging bij de invoering van elektronisch berichtenverkeer.**

## INLEIDING

Organisaties opereren in een continu veranderingsproces. Ook de bancaire sector is volop in beweging. Op internationaal niveau heeft de Europese regelgeving de liberalisatie van het geldverkeer binnen de Europese gemeenschap in een stroomversnelling gebracht. Op nationaal niveau heeft het nieuwe structuurbeleid van het ministerie van Financiën tot een brancheverwaging geleid tussen banken en verzekeringsmaatschappijen. Fusies leiden tot schaalvergrotingen gepaard gaande met scherper wordende concurrentieverhoudingen.
Om deze concurrentie het hoofd te kunnen bieden is het voor de Kas-Associatie NV (Kas-Ass) van strategisch belang gebruik te maken van de nieuwe ontwikkelingen in de informatietechnologie, Electronic Data Interchange (EDI): het elektronisch uitwisselen van gestructureerde gegevens, volgens overeengekomen berichtenstandaarden, van computerapplicatie naar computerapplicatie.
In dit artikel wordt nader ingegaan op de ontwikkeling en implementatie van EDI bij de Kas-Ass en de consequenties hiervan voor de interne controle en beveiliging.
Uitgangspunt hierbij zijn de binnen de Kas-Ass gehanteerde normen voor interne controle en beveiliging. Deze worden nader toegelicht.

## KAS-ASSOCIATIE

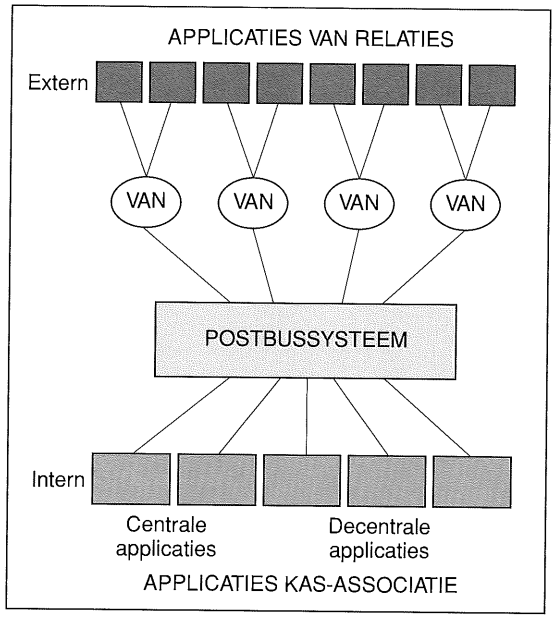
De Kas-Ass is een bankinstelling die diensten verleent aan de leden van de Vereniging voor de Effectenhandel en aan andere interprofessionele instellingen. Voortvloeiend uit haar statutaire handelsneutraliteit, inhoudende het verbod van de handel in effecten en van het optreden als emissiehuis, is de Kas-Ass zelf geen lid van de Vereniging voor de Effectenhandel. De Vereniging voor de Effectenhandel is sedert 1974 aandeelhouder van de Kas-Ass; op dit moment houdt zij 60 procent van het aandelenkapitaal. De Kas-Ass beschikt over een geavanceerd bewaarbedrijf en verzorgt de settlement (afwikkeling) van nationale en internationale effectentransacties ten behoeve van zowel binnen- als buitenlandse banken, brokers, clearing-instituten, institutionele beleggers en vermogende particulieren. Zij onderhoudt een verbruikleencircuit in aandelen en obligaties. Als bank voor de effectenhandel verzorgt zij de financiering van de effecten- en de optiehandel en het betalingsverkeer dat met de effecten- en optietransacties samenhangt. De Kas-Ass heeft ongeveer 550 medewerkers in dienst, van wie circa 100 werkzaam in de automatisering.




*Figuur 1. Ontwikkelingen in Kas-Ass EDI-systeem.*

### Ontwikkelingen

De afgelopen jaren hebben bij de Kas-Ass in het teken gestaan van interne en externe integratie. Het doel van de interne integratie is, door een optimalisatie van de bestaande kernsystemen (het effectensysteem, het geldsysteem en het optiesysteem), te komen tot een meer geïntegreerde bedrijfsvoering. Door specifieke eisen en wensen van cliëntengroepen en als gevolg van technologische ontwikkelingen is tevens een sterke tendens ontstaan naar externe integratie (zie de figuren 1 en 2). In 1987 introduceerde de Kas-Ass een EDI-systeem ten behoeve van haar cliënten onder de naam DECK (Distributie en Collectie van Kas-Ass-informatie). Dit EDI-systeem werd gerealiseerd met een mainframe en een front-end processor. Hierbij werd een verbinding gelegd tussen het mainframe en dit DECK-systeem (de "overslagcomputer"). Dit laatste systeem regelt de informatie-uitwisseling tussen de Kas-Ass en haar cliënten.
Door interne en externe factoren is in 1990 besloten een nieuw systeem te ontwikkelen, het *postbussysteem* "PB".

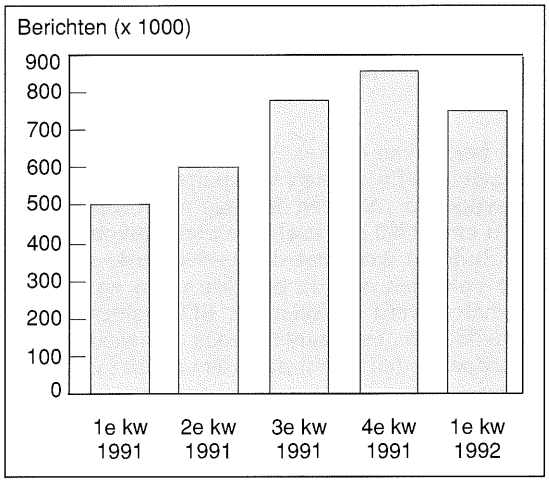



*Figuur 2. Introductie van het PB-systeem.*

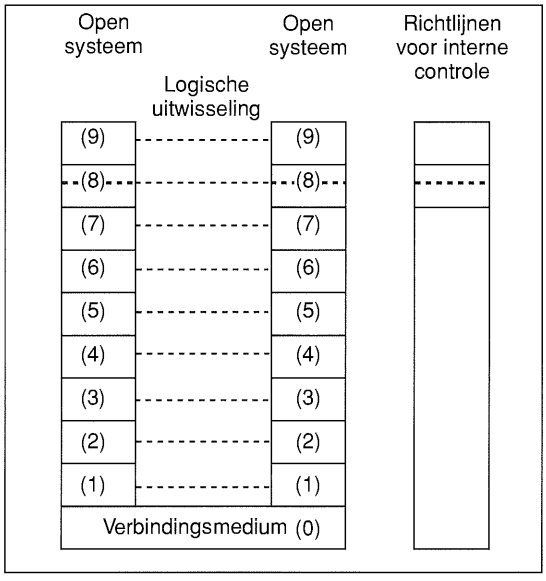
De belangrijkste interne factor is dat, door de stormachtige toename van het aantal berichten, de hardware-interface de grens van zijn maximumcapaciteit had bereikt (zie figuur 3). Bovendien nam het aantal ontwikkelde of gekochte applicaties, zowel centraal als decentraal, fors toe. Omdat deze applicaties ook onderling met elkaar communiceren steeg de behoefte aan een "postbezorging". Een belangrijk voordeel hierbij is dat de gegevensuitwisseling tussen de bestaande applicaties in sterke mate wordt vereenvoudigd.

De behoeften van de cliënten aan een effectieve en efficiënte communicatie en de opkomst van "Value Added Network-services" zijn de belangrijkste externe factoren die de ontwikkeling van een PB-systeem een positieve impuls hebben gegeven.

Het PB-systeem heeft inmiddels 75 postbussen. Met een volume van circa drie miljoen berichten per jaar behoort de Kas-Ass, volgens een laatste EDIFORUM-enquête, tot de EDI top vijf van Nederland.




*Figuur 3. Overzicht aantal berichten per kwartaal.*




*Figuur 4. OSI-referentiemodel.*

## BEGRIPSAFBAKENING EDI

In het door de ISO (International Standardization Organization) ontwikkelde Open Systems Interconnection (OSI) Reference Model worden zeven lagen in het netwerkmodel onderscheiden. Dit OSI-referentiemodel is een model van functies voor communicatie tussen twee computersystemen en heeft een gelaagde structuur. Deze lagen zijn schematisch weergegeven in figuur 4.

Voor de beeldvorming en de afbakening van het onderwerp van dit artikel zijn aan dit OSI-model twee lagen toegevoegd:

- Laag 8, de EDI-laag, is verantwoordelijk voor de gestructureerde uitwisseling en buffering van de EDI-berichten. Deze laag wordt bij de Kas-Ass gevormd door het PB-systeem.

- Laag 9 zijn de toepassingen, in het OSI-referentiemodel aangeduid als Applicatieprocessen. Dit zijn bij de Kas-Ass de effectensystemen, geldsystemen en optiesystemen.

De onderliggende lagen worden in dit artikel niet behandeld.

## DEFINITIE EDI

In de EDI Control Guide [EDIC90] wordt de volgende definitie gehanteerd: "EDI is the process of transferring information from one company's computer to another company's computer, in a standard format, so the receiving company understands the sending company's requirements and is able to act on them".

Trefwoorden voor bovenstaande definitie zijn standaardisatie en gegevensuitwisseling tussen computersystemen. Omdat de vorm en de volgorde waarin de gegevens worden uitgewisseld niet vrij zijn, vallen andere vormen van elektronisch communiceren, zoals electronic mail, niet onder EDI.

Standaarden voor het berichtenverkeer in het bankbedrijf zijn nog in ontwikkeling. Op initiatief van de Beleidscommissie Informatica/Telematica van de Nederlandse Vereniging van Banken is in het najaar van 1990 de Commissie EDI geformeerd om te adviseren over de vormgeving en inrichting van interbancaire samenwerking bij Electronic Data Interchange voor de financiële berichtgeving tussen banken en bedrijven. Onder toezicht van de Nederlandse Vereniging van Banken is op 8 mei 1991 het projectbureau EDIFIST opgericht. De Commissie heeft in het rapport "Electronic Data Interchange: Contouren voor een interbancaire EDI-infrastructuur" een advies uitgebracht. De belangrijkste conclusie in dit advies is dat interbancaire EDI-structuur noodzakelijk is om financiële EDI-berichten, gebaseerd op de EDIFACT-standaard, tussen banken en handelspartners te kunnen uitwisselen.
In de eerste fase komt deze infrastructuur met name beschikbaar ten behoeve van het nationale en internationale betalingsverkeer. In een latere fase zullen naar verwachting ook andere toepassingen via deze interbancaire EDI-infrastructuur verwerkbaar worden: toepassingen op het gebied van documentaire kredietverlening, dienstverlening op het terrein van factoring, het automatiseren van het documentenverkeer in verband met de betalingsbalansrapportage en in een later stadium applicaties voor de effectenhandel.

## KENMERKEN VAN EEN POSTBUSSYSTEEM

Voor de beeldvorming van een *postbussysteem* trekken we een parallel met de verwerking van de partijenpost door de PTT. De verantwoordelijkheden zijn hierbij duidelijk afgebakend:
De cliënt biedt de partijenpost gebundeld en in zakken aan bij het lokale postkantoor. Dit geschiedt conform de PTT-voorschriften met betrekking tot de adressering, de bestemming, de afzender, het formaat van de enveloppe en de frankering.

*Elke organisatie kent haar eigen normen voor de integratie van berichten. Hierbij is het van belang dat de definitie van gegevenselementen die een organisatie gebruikt, is afgestemd op de internationaal gehanteerde definities.*

De PTT transporteert de postzak naar het postverdeelcentrum, schudt de postzakken leeg en controleert de adressering, bundeling en frankering. De poststukken worden gesorteerd en afgelegd in de postbus van de geadresseerde. Verder stelt de PTT de post beschikbaar aan de geadresseerde door de post te bezorgen of af te laten halen uit de postbus. De PTT neemt maatregelen tegen het zoek raken van de post en het ongeoorloofd openen van de post en is verantwoordelijk voor de continuïteit van de dienstverlening.

De bovengenoemde verantwoordelijkheden van de PTT geven de systeemcomponenten van het PB-systeem weer:
- uitvoeren van een aantal controles; in de paragraaf Interne controle wordt hierop nader ingegaan;
- het plaatsen van het bericht in de postbus van de geadresseerde;
- het bevestigen van de goede ontvangst aan de afzender;
- het treffen van voorzieningen met betrekking tot de beveiliging, backup/recovery en de uitwijk.

De doelstelling van het PB-systeem is tweeledig: het verzorgt de communicatie tussen interne en externe computersystemen en het mainframe, en het vormt de interface tussen de applicaties op het mainframe.

## WERKWIJZE ONTWIKKELING NIEUW SYSTEEM

Het beleid van de Kas-Ass is erop gericht, indien mogelijk, software aan te schaffen en niet zelf te ontwikkelen. Na een strenge selectieprocedure heeft eind 1990 een evaluatie plaatsgevonden. Geconcludeerd werd dat de geselecteerde systemen niet voldeden aan de gestelde eisen en wensen. Derhalve werd besloten het EDI-systeem zelf te ontwikkelen. Een aantal reeds aanwezige standaardpakketten vormt de basis van dit systeem, te weten:
- een spool-pakket, dat binnen PB fungeert als een "postverdeelcentrum" voor het verdelen van de berichten over de postbussen;
- een toegangsbeveiligingssysteem (TBS), dat zorg draagt voor de identificatie, authenticatie en autorisatie van gebruikers en processen;
- een communicatiepakket, dat de communicatie verzorgt met niet mainframe-applicaties.

Aanvullend op deze standaardpakketten is een gering aantal programma's ontwikkeld voor het doen samenwerken van bovengenoemde systemen als één PB-systeem. Programmeurs met een specialistische kennis van het TBS en het spool-pakket hebben het systeem gebouwd. De kern van het systeem bestaat uit elektronische postbussen. Een gebruiker kan zijn elektronische postbus selectief, per berichtsoort, legen en elektronische berichten sturen naar de elektronische postbussen van de aangesloten gebruikers. Het systeem is een "passief" systeem, dat wil zeggen het neemt zelf geen initiatief voor het opbouwen van een verbinding. Dit in tegenstelling tot de interfaces voor de berichtuitwisseling met Value Added Network-services zoals SWIFT.

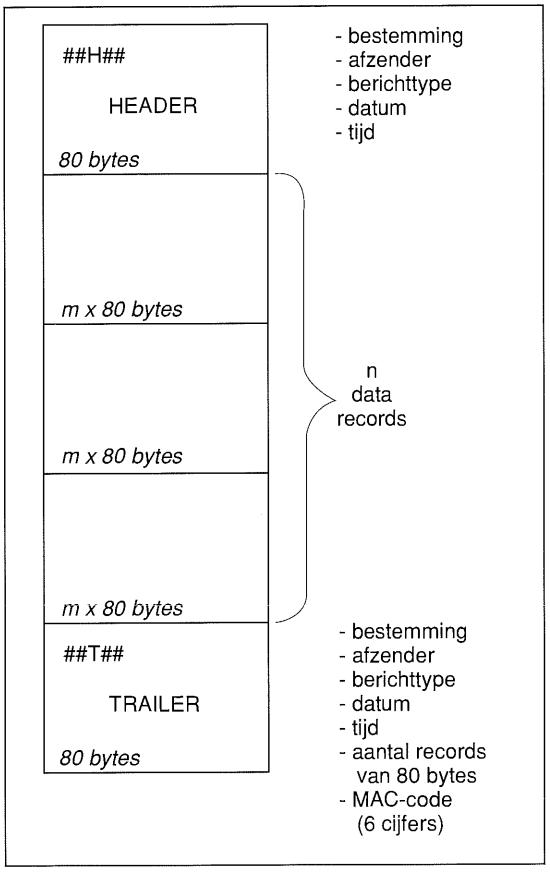
## NORMEN

Zoals uit de definitie blijkt vormen de normen voor EDI een essentieel onderdeel. Normen zijn relevant voor de integratie en berichtdefinitie.

Elke organisatie kent haar eigen normen voor de integratie van berichten. Hierbij is het van belang dat de definitie van gegevenselementen die een organisatie gebruikt, is afgestemd op de internationaal gehanteerde definities. Hierdoor worden begripsverwarring en conversie voorkomen. De Kas-Ass conformeert zich aan de internationaal ontwikkelde standaarden. Voorbeelden hiervan zijn de fondscoderingen en de muntcoderingen.

De basis voor de berichtdefinitie in het PB-systeem vormen de data-elementen; deze worden voor de informatie-overdracht op een "logische wijze" gestructureerd tot records (segmenten). Deze segmenten worden op hun beurt weer gegroepeerd tot berichten. Deze berichten worden herkend aan de hand van specifieke "stuursegmenten" zoals een message header (het start-segment) en een message trailer (het afsluitend segment).

In de message header zijn gegevens opgenomen met betrekking tot de afzender, de geadresseerde, het berichttype, de datum en de tijd.
In de message trailer is een aantal gegevens opgenomen voor interne controledoeleinden, zoals een Message Authentication Code en het totaal aantal records.
De data records bevinden zich tussen de header en de trailer. De opbouw van de data records is afhankelijk van het informatietype. Inmiddels zijn ruim vijftig informatietypen ontwikkeld voor geld-, optie- en effectenberichten. Voorbeelden hiervan zijn de geldoverboekingsopdrachten en de girale effectenoverboekingsopdrachten (zie figuur 5).




*Figuur 5. Berichtenstructuur.*

| van \ naar | CA | DA | EA | IF |
|---|---|---|---|---|
| CA | X | X | X | X |
| DA | X | X | X | X |
| EA | X | X | X | — |
| IF | X | X | — | — |

*Tabel 1. Informatiestromen PB-systeem.*

*Toelichting*
CA Centrale Applicaties op het mainframe binnen de Kas-Ass;
DA Decentrale Applicaties binnen de Kas-Ass (PC/mini's);
EA Externe Applicaties van relaties;
IF Interfaces met Value Added Network-services.

## RISICO-ANALYSE

Op basis van een inventarisatie van de risico's is beoordeeld in hoeverre adequate maatregelen van interne controle en beveiliging zijn genomen.

Voorwaarde voor een risico-analyse is een beleid met betrekking tot de toegestane informatiestromen.

Uit de matrix in tabel 1 kunnen we concluderen dat het beleid van de Kas-Ass erop gericht is elke vorm van communicatie-uitwisseling te ondersteunen met uitzondering van berichtuitwisseling van externe applicaties via de interfaces naar andere externe applicaties.

Het beleid ondersteunt wel de berichtuitwisseling tussen cliënten onderling. De Kas-Ass treedt in dit geval op als een Value Added Network-service voor externe cliënten.

Risico's met betrekking tot EDI (zie figuur 4, laag 8 van het model) kunnen we onderscheiden in risico's met betrekking tot de integriteit (juistheid, tijdigheid, volledigheid) van de gegevensuitwisseling, de beschikbaarheid en de exclusiviteit.

Als risico's met betrekking tot de integriteit kunnen worden genoemd: de berichten komen in een verkeerde postbus of verkeerd postvak; de berichten worden aan een verkeerde applicatie gestuurd; de berichten komen niet op tijd of dubbel in een postbus/postvak; de berichten worden dubbel uit een postvak gehaald of verdwijnen uit het postvak.

Het risico voor wat betreft de beschikbaarheid is dat het PB-systeem of de daarbij behorende communicatie-software niet beschikbaar is.

Als risico-elementen met betrekking tot de exclusiviteit zijn te noemen: de berichten worden door niet-geautoriseerde gebruikers gedeponeerd in een postbus/postvak; de berichten worden tijdens de behandeling door PB door ongeautoriseerde medewerkers gelezen/gemuteerd; de berichten hebben een onbekende afzender; de berichten worden door een niet-geautoriseerde gebruiker uit een postvak verwijderd.

De basis voor de getroffen maatregelen van interne controle en beveiliging is verwoord in een beveiligingsbeleid; dit laatste is gebaseerd op een verant-

woord evenwicht tussen enerzijds de noodzaak tot beveiliging en interne controle en anderzijds de financiële consequenties. Een onderdeel van dit beleid wordt gevormd door de richtlijnen van interne controle en beveiliging.

*De basis voor de getroffen maatregelen van interne controle en beveiliging is verwoord in een beveiligingsbeleid; dit laatste is gebaseerd op een verantwoord evenwicht tussen enerzijds de noodzaak tot beveiliging en interne controle en anderzijds de financiële consequenties.*

## ALGEMENE RICHTLIJNEN VOOR DE BEVEILIGING

De belangrijkste doelstelling van beveiliging is bescherming te bieden tegen van binnen en van buiten komend onheil. De richtlijnen om dit te ondersteunen kennen onder meer de volgende elementen:

- Persoonlijke verantwoordelijkheid; dat wil zeggen systemen moeten dusdanig zijn ontworpen dat de gepleegde handelingen kunnen worden herleid naar een verantwoordelijke medewerker.

- De door automatisering ondersteunde functiescheidingen.

- De technische handhaving van de functiescheidingen en niet op basis van procedurele maatregelen.

- Spelregels voor een standaardnaamgeving. Elk systeem dient te voldoen aan de naamgevingsstandaard. Door gebruik te maken van deze standaard moet het mogelijk zijn alle relevante resources van een systeem te beveiligen.

- Spelregels voor de identificatie, authenticatie en autorisatie. Bij toegangsbeveiliging gaat het in feite om twee zaken. In de eerste plaats om te voorkomen dat ongeautoriseerde personen toegang krijgen tot het computersysteem en in de tweede plaats om te voorkomen dat personen die rechtens toegang hebben tot het systeem met dat systeem handelingen uitvoeren die niet in overeenstemming zijn met hun functie. Een beveiligd systeem vraagt naar de identiteit van degene die toegang zoekt. De identiteit van elke gebruiker is in het systeem vastgelegd met de user-id, een acroniem van de naam van de gebruiker (identificatie). Vervolgens zal degene die toegang zoekt, moeten aantonen dat hij werkelijk degene is voor wie hij zich uitgeeft (authenticatie). Het systeem vraagt om een bewijs, de persoon levert dit door een "password" in te voeren. Elke behandeling waarbij gegevens worden benaderd, wordt door het systeem gecontroleerd. De bevoegdheden behoren in overeenstemming te zijn met de functie die hij uitoefent; ze zijn in het systeem vastgelegd in een "profile" en aan het user-id gekoppeld (autorisatie).

- Systemen bouwen geen eigen beveiligingsomgeving op.

- De personal computers die beschikken over een mainframe-aansluiting zijn niet voorzien van diskettestations.

- De beveiliging van personal computers gekoppeld aan het mainframe is gebaseerd op het TBS, het communicatiepakket en een lokaal draaiend beveiligingssysteem.

## ALGEMENE RICHTLIJNEN VOOR DE INTERNE CONTROLE

Interne controle wordt gerealiseerd door in de applicatie maatregelen op te nemen die ervoor zorgen dat deze tijdens het functioneren aan de doelstelling beantwoordt.
Te noemen in dit verband zijn onder andere de volgende richtlijnen met betrekking tot:

- De *juistheid:* dat wil zeggen dat de gegevens een juiste weergave moeten zijn van de werkelijkheid. Deze controles bestaan uit validaties en, indien mogelijk, inhoudelijke controles of de gegevens overeenstemmen met het brondocument. Daarnaast wordt aan de hand van de doorlopende nummering een controle op dubbele berichten uitgevoerd.

- De *volledigheid:* het systeem moet signaleren of posten ontbreken (volgnummering). Het "ontvangende systeem" heeft hierbij de taak de volledige ontvangst van de gegevens vast te stellen, terwijl het aanleverende systeem de juiste gegevens hiervoor ter beschikking moet stellen ("netwerk van controletotalen").

- De *tijdigheid:* de gegevens in het systeem die worden beheerd, moeten een actuele afbeelding zijn van de werkelijkheid. Deze controles moeten voorkomen dat de gegevens verouderen en databases vervuilen.

- De *continuïteit:* maatregelen moeten aanwezig zijn die erop gericht zijn dat een continu functioneren mogelijk is (aspecten van onderhoudbaarheid, backup/restore-, recovery- en herstartprocedures).

- Het *beheer:* het systeem moet maatregelen bevatten die de gebruiker en de beheerder informatie verschaffen die zij nodig hebben voor hun werk-

zaamheden. Deze informatie dient tevens als bewijsmateriaal op grond waarvan zij verantwoording van het gebruik en beheer kunnen afleggen (ter verkrijging van decharge).

– De *audit trail:* het systeem moet een audit trail opbouwen om te kunnen vaststellen welke gebruiker op welk moment welke handeling heeft uitgevoerd. De verstrekte informatie mag geen individuele posten of posten in totalen bevatten die onverklaarbaar en niet traceerbaar zijn.

Achtereenvolgens wordt een aantal getroffen maatregelen van beveiliging en interne controle bij de ontwikkeling van het PB-systeem behandeld.

## BEVEILIGINGSMAATREGELEN POSTBUSSYSTEEM

Binnen de getroffen beveiligingsmaatregelen worden de volgende niveaus onderkend:

1. Het maken van de fysieke verbinding tussen de externe computer en de Kas-Ass. Deze kiesverbinding wordt uitsluitend tot stand gebracht via een bij de Kas-Ass geïnstalleerd terugbelsysteem. De cliënt identificeert zich met zijn gebruikersnummer. Indien dit gebruikersnummer bekend is, wordt de verbinding tijdelijk verbroken en het terugbelsysteem belt vervolgens het corresponderende telefoonnummer terug.

2. Nadat de verbinding is gemaakt, moet de "afzender" zich bekend maken bij het TBS door middel van een user-id en een password. Hierop zijn de standaard security-regels van toepassing, zoals het ten minste eenmaal per maand wijzigen van het password, de standaardnaamgeving voor de user-id, en het na een aantal foutieve inlog-pogingen blokkeren van de gebruiker.

3. Een controle of de afzender het berichttype wel aan de geadresseerde mag versturen.

Als de bovengenoemde niveaus goed zijn doorlopen, wordt het bericht in het postvak van de geadresseerde geplaatst.
Systeemtechnisch gezien houdt bovenstaande in dat de gebruiker "afzender" moet worden geautoriseerd voor de "faciliteit" postbus en voor het plaatsen van het bericht in de postbus en het postvak van de gebruiker "geadresseerde". Op gebruikersniveau moet worden bijgehouden of de gebruiker bevoegd is berichten uit het postvak te halen en/of berichten in het postvak van de geadresseerde te deponeren. Dit "gelaagde" beveiligingsniveau is gerealiseerd door naast de faciliteiten van het TBS aanvullende beveiligingsmaatregelen te treffen in het PB-systeem. Deze maatregelen zorgen ervoor dat zowel de autorisaties als de "routing" adequaat worden geregeld. Procedures in de administratieve organisatie ondersteunen deze automatiseringstechnische maatregelen.

## INTERNE CONTROLEMAATREGELEN BIJ HET POSTBUSSYSTEEM

Een belangrijk uitgangspunt voor de interne controlemaatregelen in het PB-systeem vormen de reeds aanwezige interne controlemaatregelen in de bestaande lagen van het OSI-model. Voor de functionaliteiten van het PB-systeem dienen specifieke maatregelen van interne controle te worden ontwikkeld. In figuur 4 is dit weergegeven door laag 8 in het "controleblok". De inhoud van de berichten is transparant of in PTT-jargon: het PB-systeem heeft "geen boodschap aan de boodschap". De volgende maatregelen zijn getroffen:

– Verwerkbaarheidscontroles: dit zijn de syntaxcontroles op de header- en trailer-informatie.

– Controle op de autorisaties: dit aspect is reeds in de paragraaf over beveiliging behandeld.

– Maatregelen met betrekking tot de continuïteit. Uitgangspunt hierbij is dat geen berichten verloren mogen gaan. Een bericht wordt geacht te zijn ontvangen door de Kas-Ass op het moment dat de bevestiging van opslag in de PB is afgegeven aan de afzender. Berichten worden op twee fysiek gescheiden schijven vastgelegd in software-matig gescheiden postbussen. Op vaste tijden worden backups gemaakt op tape. Het PB-systeem kent een checkpoint-mechanisme zodat na een systeemstoring een automatische recovery plaatsvindt. Indien door een calamiteit het mainframe en dus het PB-systeem voor langere tijd niet beschikbaar is, wordt gebruik gemaakt van de standaarduitwijkprocedure.

– Maatregelen met betrekking tot het beheer. In de volgende paragraaf wordt hierop nader ingegaan.

*Interne controle wordt gerealiseerd door in de applicatie maatregelen op te nemen die ervoor zorgen dat deze tijdens het functioneren aan de doelstelling beantwoordt.*

– Maatregelen met betrekking tot de audit trail. Door het PB-systeem wordt elke handeling vastgelegd. Omdat het PB-systeem grotendeels op standaardpakketten is gebaseerd, is de logging verschillend van aard. Dit heeft consequenties voor het beheer omdat specifieke kennis van de pakketten vereist is.

De log-informatie is gedurende de daguren online opvraagbaar. Log-informatie kan door de beheer-

der als "bericht" naar het desbetreffende postvak worden gestuurd om van daaruit naar een lokale of remote printer te worden gestuurd.

## BEHEER VAN DE POSTBUS

Elke laag van het OSI-model vereist andersoortig beheer. Onderstaand wordt nader ingegaan op het beheer van laag 8.

**Beheer van de autorisatie**

Het beheer van de autorisatie beperkt zich niet slechts tot de grenzen van het beveiligingspakket. Ook de aanvullende systeemtechnische en procedurele maatregelen met betrekking tot de autorisaties van afzender, het berichttype, de postbus en het postvak en een indicatie of de gebruiker het postvak mag leeghalen of vullen, vormen een onderdeel van dit beheer.

**Beheer van het PB-systeem**

Het beheer van de postbus is ondergebracht bij een speciale EDI-groep, de groep Informatie Distributie (ID). Dit beheer steunt in belangrijke mate op automatiseringstechnieken.

*De ontwikkeling en het gebruik van EDI is een leerproces dat elk bedrijf proefondervindelijk moet ondergaan.*

Berichten worden, na ontvangst door de geadresseerde, uit het postvak verwijderd. Een duplicaat van het bericht blijft nog zeven dagen beschikbaar in de postbus van de beheerder voor eventuele hertransmissie. Na deze termijn worden berichten op magneetband gearchiveerd.

**Change management**

We kunnen bij change management onderscheid maken tussen de invoer van nieuwe of wijziging van bestaande postbus-cliëntgegevens en/of het initiëren van een nieuw informatietype via het PB-systeem. Het signaal hiervoor komt in eerste instantie van de account manager. Op basis van een primaire vastlegging voert de groep ID de gegevens in.

Een nieuw informatietype heeft niet slechts consequenties voor PB maar evenzeer voor de toepassingen (laag 9). Aanpassingen hierin geschieden conform een standaardaanvraagprocedure.

**Gegevensmanagement**

De belangrijkste taak van gegevensmanagement is het definiëren en onderhouden van standaardberichttypen. Tijdens de introductie van het postbusconcept waren nog geen bancaire EDI-standaarden voor berichtuitwisseling aanwezig. Ontwikkelingen hieromtrent zijn sinds kort gaande.

## SAMENVATTING

Het bankbedrijf bevindt zich in een dynamische omgeving waarin voortdurend op veranderingen moet worden ingespeeld. Cliënten eisen snelle en betrouwbare informatie; de servicegraad van banken vormt derhalve een kritische succesfactor. De Kas-Ass heeft hierop geanticipeerd met de ontwikkeling van een EDI-toepassing, het postbussysteem, waardoor de beoogde bedrijfsdoelstellingen, gericht op produkt- en marktontwikkelingen, mede kunnen worden gerealiseerd. Hierbij is grote aandacht geschonken aan de beveiliging, interne controle en beschikbaarheid van het systeem.

## CONCLUSIE / AANDACHTSPUNTEN

- De ontwikkeling en het gebruik van EDI is een leerproces dat elk bedrijf proefondervindelijk moet ondergaan. De technische infrastructuur is, in de vorm van het postbussysteem, inmiddels voorhanden. De aansluiting van deze EDI-toepassing met de bancaire toepassingen, in figuur 4 weergegeven door het grensvlak tussen de lagen 8 en 9, is complex en tijdrovend.

- Standaarden voor EDI-toepassingen in het bankbedrijf zijn nog in ontwikkeling. In maart 1992 heeft een EDI-commissie onder auspiciën van de Nederlandse Vereniging van Banken een eindadvies uitgebracht "Electronic Data Interchange: Contouren voor een interbancaire EDI-infrastructuur". De belangrijkste conclusie in dit eindadvies is dat een interbancaire EDI-infrastructuur noodzakelijk is om financiële EDI-berichten die voldoen aan de internationale EDIFACT-standaard, tussen banken en handelspartners te kunnen uitwisselen. Standaarden met betrekking tot effectenberichten zijn vooralsnog niet aanwezig.

- Elke laag in het OSI-model vereist specifieke maatregelen van interne controle en beveiliging. De EDI-laag moet in belangrijke mate kunnen steunen op de getroffen maatregelen in de overige lagen. In het postbussysteem zijn specifieke maatregelen geprogrammeerd die door procedurele maatregelen in de administratieve organisatie worden ondersteund.

- De Kas-Ass heeft, na een uitgebreide selectieprocedure, destijds gekozen om het postbussysteem zelf te ontwikkelen. De fundamenten hiervoor waren reeds aanwezig in de vorm van een toegangsbeveiligingssysteem en een spool-pakket.

Een vereiste hierbij is dat de ontwikkelaars een specialistische en verregaande kennis bezitten van deze pakketten om interface- en communicatieproblemen tussen de pakketten op te lossen. Ook voor het beheer van het postbussysteem is het een vereiste dat voldoende kennis van deze systemen aanwezig is.

– Het ontwikkelde postbussysteem vereist specifieke beveiligingsmaatregelen. Zo moet de afzender niet alleen worden geautoriseerd voor de "faciliteit" postbus maar eveneens voor het plaatsen van het bericht in de postbus van de geadresseerde; hiernaast moet de gebruiker worden geautoriseerd om berichten uit het postvak te halen en/of berichten in het postvak van de geadresseerde te deponeren. Aanvullende maatregelen, zowel automatiseringstechnisch als procedureel, zijn binnen het postbussysteem getroffen om te kunnen voldoen aan het vereiste niveau van beveiliging.

## LITERATUUR

[EDIC90] EDICA, *EDI Control Guide*, EDI Council of Australia and the EDP Auditors Association, 1990.

[NGI89] NGI, *Beveiliging bij datacommunicatie*, rapport van het Nederlands Genootschap van Informatici, sectie Beveiliging, Kluwer Bedrijfswetenschappen, Deventer 1989.

[CEDI92] Commissie EDI, *Electronic Data Interchange: Contouren voor een interbancaire EDI-infrastructuur*, 1992.

*P. van Berge*
*Is sedert medio 1978 in dienst bij de Kas-Associatie. Tot 1987 is hij werkzaam geweest bij de afdeling Systeemontwikkeling, als systeemontwerper en informatie-analist. Tevens heeft hij enige tijd gefunctioneerd als teamleider onderhoud van de systeemgroep Effecten. Halverwege 1987 is hij overgestapt naar de Interne Accountants Dienst/EDP audit. Hij is op dit moment werkzaam als senior system EDP-auditor met als belangrijkste werkvelden de applicatieve systemen in ontwikkeling en het onderhoud hiervan.*
*Met betrekking tot het eerste veld participeert hij in een groot aantal projecten met interne controle en beveiliging als aandachtsgebied.*

# Beheersbaarheid van het EDI-verkeer in de praktijk

G.J. Endenburg RI

**Risico's die met EDI samenhangen kunnen voor een groot deel worden opgevangen in de techniek. Maar in welke mate bieden technische oplossingen zekerheid?**
**Endenburg gaat in op de beheersing van het elektronisch berichtenverkeer, waarbij de techniek centraal staat.**

## INLEIDING

Bij Europe Combined Terminals BV (ECT) begint het EDI-tijdperk nu pas goed! Steeds meer bedrijven zien de voordelen van EDI en zijn ook in staat EDI te integreren in hun bestaande of nieuw ontwikkelde informatiesystemen. Voor het management spelen, naast kostenbesparingen, commerciële motieven een belangrijke rol bij hun beslissing over het toepassen van EDI. Immers, koppeling van het eigen systeem met dat van de klant betekent toch extra dienstverlening en klantenbinding. Er zijn nu enkele EDI-projecten in ontwikkeling, waarbij de informatiesystemen van verschillende organisaties en bedrijven binnen de bedrijfskolom door middel van EDI aan elkaar gekoppeld zullen worden. Dit laatste wordt ook wel "integrale keteninformatisering" genoemd. Kortom, het EDI-verkeer neemt toe in hoeveelheid berichten, maar ook de hoeveelheid verschillende berichtsoorten en de hoeveelheid verschillende relaties waarmee EDI-berichten worden uitgewisseld, nemen toe.

## EDI BIJ ECT

Naarmate het EDI-verkeer toeneemt, neemt ook de complexiteit toe en wordt op een bepaald moment de beheersbaarheid van het EDI-verkeer een probleem. Een bedrijf zet vaak zijn eerste stappen op het EDI-toneel door te beginnen met één enkel type EDI-bericht in samenwerking met één enkele partner, zo ook bij ECT.
In eerste instantie wordt er offline getest, dat wil zeggen, al het EDI-verkeer wordt lokaal op een PC afgehandeld, zonder koppeling met het interne computersysteem. Na ontvangst van een bericht wordt dit bericht in een voor de gebruiker leesbare vorm afgedrukt, zodat visueel kan worden gecontroleerd of de inhoud van het bericht aan de verwachtingen voldoet. Eventueel wordt besloten de berichten handmatig in te voeren in het eigen computersysteem.

Na succesvolle afsluiting van de testperiode wordt de EDI-PC aangesloten op het eigen computersysteem, waarna ontvangen en te verzenden EDI-berichten elektronisch kunnen worden doorgegeven om opnieuw invoeren te voorkomen.

Het hiervoor geschetste EDI-verkeer is handmatig goed onder controle te houden. De gebruiker maakt zelf uit of en wanneer hij berichten binnenhaalt of verzendt. De gebruiker is ook in de gelegenheid zelf de inhoud van de berichten te bekijken, waardoor hij in staat is ongewenste zaken tegen te houden.
Als hetzelfde EDI-bericht met meerdere partners moet worden uitgewisseld, kan in principe dezelfde procedure worden aangehouden, waardoor de controle over het EDI-verkeer nog steeds haalbaar is, totdat het aantal partners te groot wordt.

De laatste tijd neemt het aantal verschillende EDI-partners echter toe en tegelijkertijd wordt het aantal verschillende EDI-berichtsoorten groter, terwijl de berichten ook nog bestemd zijn voor of afkomstig zijn van verschillende inhuis-applicaties.
Op dat moment ontstaan er problemen met een handmatige procedure via een PC. De hoeveelheid berichten en partners is nu zo groot geworden dat het EDI-verkeer niet meer handmatig kan worden geregeld. Het EDI-verkeer moet dus volledig worden geautomatiseerd, bijvoorbeeld door middel van een EDI-server. Zo'n EDI-server verzorgt de vertaling van intern naar extern (EDIFACT-) formaat en vice versa, regelt de datacommunicatie met de partners, verzorgt de routing naar de inhuis-applicaties op het mainframe, etc.

## RISICOGEBIEDEN

ECT heeft vooralsnog de volgende risicogebieden van het hiervoor geschetste, grootschalige EDI-verkeer onderkend:
1. continuïteit;
2. betrouwbaarheid intern computersysteem;
3. vertrouwelijkheid;
4. bewijsvoering.

Elk van deze onderwerpen zal hieronder nader worden toegelicht. In een volgende paragraaf wordt aangegeven welke maatregelen er genomen zijn in het kader van de beheersing van het EDI-verkeer.

### Continuïteit

Zodra een bedrijfsproces voor een groot deel afhankelijk wordt van het uitwisselen van EDI-berichten met partners, komt de continuïteit van dat bedrijf in gevaar bij het uitvallen of het onbetrouwbaar worden van de EDI-verbinding.

In een handmatige situatie worden er bijvoorbeeld opdrachten afgedrukt op een printer, verzameld, gescheurd, gecontroleerd, in enveloppe gestopt, gefrankeerd en verzonden. Bij de leverancier worden de enveloppen vervolgens geopend, de opdrachten worden gesorteerd, gestempeld en naar de afdeling Orderverwerking gebracht. Op deze afdeling worden de orders gecontroleerd en in het computersysteem ingevoerd.

*Zodra een bedrijfsproces voor een groot deel afhankelijk wordt van het uitwisselen van EDI-berichten met partners, komt de continuïteit van dat bedrijf in gevaar bij het uitvallen of het onbetrouwbaar worden van de EDI-verbinding.*

Bij het grootschalig invoeren van EDI zullen zowel bij de klant als bij de leverancier bepaalde taken worden overgenomen door de automatisering.
In de postkamer en op de afdeling Orderverwerking bijvoorbeeld zal het verwerken van de opdrachten niet meer nodig zijn. Ook zullen in de computersystemen bepaalde onderdelen van de software worden vervangen door andere software. Bij de klant worden de opdrachten niet meer afgedrukt en het printprogramma en de printer worden overbodig en misschien zelfs verwijderd of elders ingezet.

De mensen krijgen op den duur een andere taakinhoud en zullen hun vaardigheid bij het verwerken van de opdrachten verliezen.

Op dat moment is de afhankelijkheid van het EDI-verkeer om opdrachten te kunnen geven of verwerken een feit en is het noodzakelijk geworden na te denken over de situatie als het EDI-verkeer onverhoopt niet of niet goed werkt. Als de storing van korte duur is, is er waarschijnlijk niet veel aan de hand. Maar als dit langer duurt, bijvoorbeeld één of meer dagen, kan de normale bedrijfsvoering danig worden verstoord.

Zodra een dergelijke kwetsbare situatie ontstaat moeten er maatregelen worden genomen om uitval van de EDI-verbinding te voorkomen. Een ongestoorde bedrijfsvoering is uiteraard van belang voor beide partijen.

*In het EDI-verkeer is de afhankelijkheid van het computersysteem van de partner ook een belangrijk aspect.*

Bij het vaststellen van de benodigde voorzieningen wordt afgewogen wat het belang is van het EDI-verkeer. In feite worden de EDI-berichten stuk voor stuk beoordeeld op het belang voor de bedrijfsvoering. Ook wordt beoordeeld hoe tijdkritisch elk bericht is en of het bijvoorbeeld mogelijk is eventueel twee dagen op een bericht te wachten. In bepaalde gevallen blijkt twee uur eigenlijk al te veel te zijn.

In het EDI-verkeer is de afhankelijkheid van het computersysteem van de partner uiteraard ook een belangrijk aspect en is het van belang afspraken te maken, zodat deze partner ook maatregelen neemt om de kwetsbaarheid van de EDI-verbinding te verkleinen. Ook als er gebruik wordt gemaakt van een netwerkdienst, waardoor het EDI-verkeer niet rechtstreeks met de EDI-partner plaatsvindt, is dit soort afspraken belangrijk. Immers, zodra de partner geen berichten meer uit het netwerk kan halen of in het netwerk kan zetten, is EDI-verkeer onmogelijk.

Gebruik van een netwerkdienst brengt ook een zeker risico met zich mee. Over het algemeen is de beschikbaarheid van de faciliteiten van een bekende netwerkdienst geen probleem, maar ook een netwerkdienst kan down gaan, waardoor de berichten niet meer kunnen worden verzonden of ontvangen. Er moet dus een alternatieve route worden afgesproken, bijvoorbeeld via een normale kieslijnverbinding rechtstreeks naar het computersysteem van de partner, dan wel naar een speciaal hiervoor aangeschafte PC.

Het belangrijkste bij dit alles is dat vooraf wordt bedacht dat er iets fout kan gaan en wat er dan moet gebeuren.

*Ter illustratie een praktijkvoorbeeld:*
Op de Maasvlakte bij Rotterdam bouwt ECT een voor een groot deel geautomatiseerde containerterminal. Hier zullen vanaf 1 januari 1993 minimaal 500.000 containers per jaar voor één bepaalde klant (Sea-Land) worden overgeslagen. De taakverdeling tussen deze klant en ECT is zodanig dat er zeer nauw moet worden samengewerkt.
De klant geeft opdrachten, welke door de geautomatiseerde kranen en voertuigen, de Automatic Stacking Cranes (ASC's) en de Automatic Guided Vehicles (AGV's), in samenwerking met de bemande voertuigen, zoals Straddle Carriers (voertuigen waarmee containers op de kade verplaatst kunnen worden) en kadekranen, onmiddellijk moeten worden uitgevoerd.

Het is in principe niet mogelijk opdrachten telefonisch of per fax door te geven. Er zou te veel tijd verloren gaan met het handmatig verwerken van de opdrachten, terwijl de foutenkans aanzienlijk is. Er is dus gekozen voor een zeer intensief EDI-verkeer tussen de computersystemen van de klant en dat van ECT. Hierbij wordt bij ECT gebruik gemaakt van een speciaal voor dit doel ingerichte EDI-server. Bij uitval van deze EDI-verbinding kunnen er door de klant geen opdrachten meer aan ECT worden doorgegeven, waardoor het in principe mogelijk is dat het werk op de terminal stil komt te liggen.

Aangezien de processen op de terminal afhankelijk zijn van computers in het algemeen en van de EDI-verbinding in het bijzonder, is er bij ECT en bij de klant, in nauwe samenwerking, een aantal maatregelen getroffen om uitval van deze verbinding zoveel mogelijk te voorkomen en om de gevolgen van onverhoopte uitval zo beperkt mogelijk te houden.

Het gaat hier om drie soorten maatregelen:
- ter voorkoming van uitval van de EDI-verbinding (preventief);
- ter vaststelling dat de EDI-verbinding niet (goed) werkt (detectief);
  en
- om de gevolgen van uitval te beperken (correctief).

Het is duidelijk dat het zowel voor ECT als voor Sea-Land van groot belang is dat de EDI-verbinding blijft werken. De hoeveelheid berichten is zo groot dat een handmatige procedure slechts korte tijd zal kunnen werken. Het hele bedrijfsproces is ontworpen voor gecomputeriseerde verwerking en, hoewel er goede handmatige procedures zijn ontwikkeld, moeten we toch ervan uitgaan dat, met name in pieksituaties, handmatig werken niet lang mogelijk zal zijn zonder ernstige verstoring van de gang van zaken, zoals onacceptabel lange wachttijden voor aan- en afleveringen via de weg.

**Betrouwbaarheid intern computersysteem**

Bij handmatige invoer en uitvoer van gegevens vindt er altijd nog een visuele controle plaats. Echt vreemde of ongewenste zaken worden er meestal wel uitgefilterd. Zodra EDI op enige schaal wordt toegepast, gaat de programmatuur eigenlijk haar eigen gang. Op zo'n moment moet de kwaliteit van de software zodanig zijn dat er geen ongewenste transacties kunnen plaatsvinden.

In een software-systeem van onvoldoende kwaliteit zouden bestellingen via een EDI-verbinding bijvoorbeeld kunnen zorgen voor te hoge of te lage voorraden, of worden er bestellingen geplaatst bij

partners waarmee disputen zijn. Er moeten dus hoge eisen worden gesteld aan de goede werking en de betrouwbaarheid van de programmatuur, aangezien er immers in principe geen visuele (menselijke) controle meer plaatsvindt.

In de "pre-EDI"-situatie worden opdrachten op papier ontvangen (brief, fax, telex). De leverancier heeft de beschikking over een afdeling Orderverwerking, waar door mensen de opdrachten worden gelezen, vergeleken met contracten, afspraken, artikellijsten, prijslijsten, en dergelijke. Hierbij kunnen ook abnormale zaken aan het licht komen, zoals het bestellen van een, voor die klant, ongewoon artikel of abnormale hoeveelheid.

Zodra een opdracht op deze manier door mensen is gecontroleerd, wordt deze handmatig ingevoerd in het computersysteem. Ook nu worden er door de programmatuur controles uitgevoerd, zoals bestaanbaarheid van artikelen, beschikbaarheid van artikelen, hoeveelheden en kredietwaardigheid van de klant.

Zodra EDI is ingevoerd, worden de opdrachten automatisch gegenereerd en naar de leverancier gestuurd. De programmatuur moet er nu voor zorgen dat geen ongewenste dingen plaatsvinden. De afnemer zal criteria moeten vaststellen, zoals tijdstip van bestellen, minimumvoorraad, bestelhoeveelheden, welke leveranciers wel en welke beslist niet, vereiste leveringstermijnen, en dergelijke.

De software aan de kant van de leverancier zal ervoor moeten zorgen dat er geen leveranties aan dubieuze debiteuren plaatsvinden, dat er signalering plaatsvindt zodra er abnormale en ongebruikelijke artikelen of hoeveelheden worden besteld, wellicht alleen in relatie tot die afnemer. En zo zijn er uiteraard veel te programmeren controles op te noemen.

Voor ECT zijn bijvoorbeeld de volgende zaken belangrijk:
- ontbrekende berichten, waardoor opdrachten niet worden uitgevoerd;
- dubbele berichten, waardoor opdrachten dubbel kunnen worden uitgevoerd;
- niet volledig verwerkte berichten, waardoor opdrachten gedeeltelijk worden uitgevoerd;
- niet (tijdig) op EDI-bericht reageren door de partner, waardoor de uitvoering van opdrachten stagneert en onnodig wachttijden ontstaan.

Deze zaken moeten worden onderkend en de gevolgen moeten worden geïnventariseerd. Ze kunnen worden veroorzaakt door fouten in de eigen programmatuur of in de programmatuur van de partner, dan wel door een hardware-storing, waardoor bijvoorbeeld niet wordt vastgelegd dat een bericht is verstuurd, terwijl dit wel het geval was.

De technische datacommunicatie tussen computersystemen kan in principe foutloos verlopen. Dit is echter geen vanzelfsprekende zaak en er zullen maatregelen moeten worden getroffen om transmissiefouten onmogelijk te maken. Ook kunnen er fouten optreden bij het aanmaken van een EDI-bericht, waardoor het ontvangende systeem niet in staat is het bericht op correcte wijze te verwerken. Als er tijdens de overdracht van EDI-berichten storingen optreden, kan het bericht door het ontvangende systeem niet worden verwerkt. Dit soort storingen kan worden veroorzaakt doordat gebruik gemaakt wordt van een minder goede telefoonverbinding.

*Het is belangrijk dat er goede en gedetailleerde afspraken worden gemaakt tussen de EDI-partners voor de situatie dat berichten in hun geheel worden afgekeurd of dat individuele records worden afgekeurd.*

Er kan met een correct gecommuniceerd EDI-bericht ook nog van alles mis zijn. Er kunnen verplichte data-elementen ontbreken, incorrecte codes worden gebruikt, verplichte segmenten of recordtypen kunnen ontbreken, etc. Het is belangrijk dat er goede en gedetailleerde afspraken worden gemaakt tussen de EDI-partners voor de situatie dat berichten in hun geheel worden afgekeurd of dat individuele records worden afgekeurd.

**Vertrouwelijkheid**

De vertrouwelijkheid van gegevens kan in gevaar komen. Tenslotte wordt er een grote hoeveelheid gegevens via datalijnen, netwerkdiensten en dergelijke uitgewisseld. Het is denkbaar dat een buitenstaander gegevens aftapt en op deze manier vertrouwelijke gegevens beschikbaar krijgt.

Het zal in de praktijk wellicht niet vaak voorkomen dat er zeer gevoelige gegevens door middel van EDI worden uitgewisseld. Toch kan het nuttig zijn eens met een kritisch oog naar de uitgewisselde EDI-berichten te kijken. De meeste mensen zullen "spionage" niet echt als een gevaar zien, maar uitgesloten is het niet. Zodra er gegevens als prijsinformatie, produktsamenstelling en dergelijke via EDI worden uitgewisseld, moet de kans op "aftappen" door een concurrent zo klein mogelijk worden gemaakt.

De vraag is dus hoeveel een concurrent ervoor over heeft gegevens over produkten, produktieproces, prijsafspraken en dergelijke te verkrijgen, welke voordelen een dergelijke kennis hem zal kunnen bieden en of hij wellicht nadeel kan berokkenen met die kennis. Ieder bedrijf zal zelf deze afweging moeten maken.

Er zijn meerdere systemen voor het versleutelen van EDI-berichten, welke ook in combinatie kunnen worden gebruikt. Zodra dit soort technieken wordt gebruikt, moeten sleutelafgifte en -beheer goed worden geregeld, opdat dit aspect niet een risico op zich wordt.

Het is helaas ook denkbaar dat een buitenstaander of zelfs een eigen werknemer bewust schadelijke gegevens, in de vorm van gefingeerde, maar voor een computer geldige EDI-berichten, aanbiedt. Hiermee zou het mogelijk zijn belangrijke gegevensbestanden zodanig te wijzigen dat ze onbruikbaar worden of zelfs verkeerd aansturen van een computerprogramma, bijvoorbeeld betalingen of facturatie, veroorzaken.

*Teneinde het intensieve EDI-verkeer in goede banen te leiden en de potentiële gevaren het hoofd te kunnen bieden is het zaak goede, professionele EDI-voorzieningen aan te brengen.*

Zodra betalingen via EDI-berichten naar de bank worden gestuurd, moet ervoor worden gezorgd dat alleen geautoriseerde betalingen door de bank zullen worden verwerkt. Buitenstaanders of onbevoegde personeelsleden mogen nooit in staat zijn een geldige doch gefingeerde betalingsopdracht via EDI aan de bank te sturen. Ook zal moeten worden voorkomen dat buitenstaanders opdrachten kunnen onderscheppen en in gewijzigde vorm doorsturen.

Het is dus noodzakelijk de inkomende en uitgaande fraudegevoelige berichten te identificeren, waarna maatregelen kunnen worden genomen om fraude te voorkomen. In dit verband is het dus noodzakelijk zekerheid te verkrijgen dat een dergelijk bericht daadwerkelijk door een geautoriseerd persoon werd verzonden en dat de belangrijke gegevens, zoals hoeveelheden, bedragen en dergelijke, kloppen.

**Bewijsvoering**

Specifiek kenmerk van EDI-verkeer is dat er geen papier aan te pas komt. Het op papier afdrukken van een EDI-bericht in de vorm waarin dit wordt ontvangen of verzonden, is zeer ongebruikelijk en uiteraard ongewenst. Tenslotte is het de bedoeling alle transacties elektronisch af te wikkelen, zonder papieren documenten. Zodra zich echter een dispuut voordoet, bijvoorbeeld over bestelde hoeveelheden (klant zegt 100 stuks besteld te hebben, terwijl het eigen systeem 1000 stuks heeft geregistreerd), dan is het moeilijker aan te tonen hoe het bericht er heeft uitgezien.

In een conventionele situatie zullen belangrijke berichten, zoals bestellingen, opdrachten en dergelijke, schriftelijk worden gegeven, voorzien van de handtekening van een bevoegd persoon. Deze handtekening kan worden vastgelegd en door de ontvanger eventueel worden gecontroleerd met de handtekeningen in het handelsregister van de Kamer van Koophandel. Hier gaat een duidelijke bewijskracht van uit.

Zodra dit soort berichten via EDI wordt verstuurd, kunnen de berichten worden voorzien van een elektronische handtekening. Echter, vooral als het om grote hoeveelheden routineberichten gaat, wordt er meestal voor gekozen dit achterwege te laten, omdat het te omslachtig is. In dit soort gevallen is het van belang het EDI-bericht in de vorm waarin het is ontvangen, te bewaren als bewijsvoering. Hoewel er nog geen echte wettelijke voorschriften zijn, wordt in de praktijk ervan uitgegaan dat de regels voor papieren documenten hier eveneens van toepassing zijn. Dat wil zeggen, EDI-berichten moeten tien jaar worden bewaard en zullen eventueel moeten worden gereproduceerd.

Dit uitgangspunt heeft nogal wat technische en organisatorische consequenties. Het is de vraag of een bepaald medium, zoals tape, tien jaar goed blijft. De tapes moeten dus regelmatig worden ververst, ook als de tape-unit wordt vervangen.
Verder is de bewijskracht van EDI-berichten zeer klein, vergelijkbaar met die van faxen en telexen. Er kan immers mee worden gemanipuleerd. Toch vindt de wetgever (Wetboek van Koophandel) dat faxen en telexen tien jaar moeten worden bewaard. Zodra er namelijk een dispuut ontstaat is het wellicht mogelijk, aan de hand van een gearchiveerd bericht (fax, telex of EDI-bericht), de tegenpartij ervan te overtuigen dat hij ongelijk heeft. Op dit moment zal een te goeder trouw zijnde tegenpartij waarschijnlijk besluiten af te zien van een rechtszaak.

## ECT EDI-SERVER

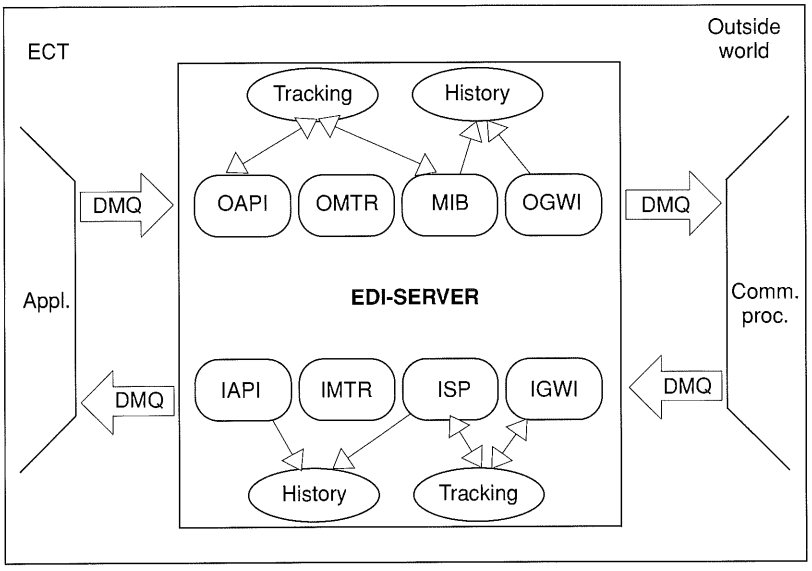
Teneinde het intensieve EDI-verkeer in goede banen te leiden en de genoemde potentiële gevaren het hoofd te kunnen bieden is het zaak goede, professionele EDI-voorzieningen aan te brengen. Het systeem met dit soort voorzieningen wordt bij ECT "EDI-server" genoemd. Hieronder volgt een beschrijving van de functionaliteiten van deze EDI-server van ECT.

De EDI-server heeft tot doel de diverse systemen van ECT op eenduidige wijze te voorzien van professionele EDI-faciliteiten. Hiermee worden de speciale EDI-voorzieningen, zoals vertaling, conversie en datacommunicatie, eenmalig ontwikkeld en operationeel gemaakt. De EDI-voorzieningen in de applicaties kunnen zich hierdoor in principe beperken tot het aanmaken en verwerken van inhuisbestanden. Installatie, beheer, onderhoud en gebruik van de EDI-voorzieningen worden op deze wijze eenvoudiger en goedkoper, terwijl ECT haar klanten op professionele wijze van dienst kan zijn.

De EDI-server is derhalve een interface met de buitenwereld en bestaat uit een aantal losstaande, maar nauw met elkaar samenwerkende, modules. Hierdoor kunnen respectievelijk vanuit en door de diverse ECT-applicaties EDI-berichten op eenduidige wijze worden aangeboden en verwerkt.

De EDI-server verricht de volgende hoofdtaken:
- vertaling van inhuis-formaat naar extern (EDIFACT-)formaat en vice versa;
- code-conversie;
- routering van te verzenden en ontvangen berichten;
- communicatie met de buitenwereld;
- communicatie met de applicaties;
- archivering;
- beveiliging.

Schematisch ziet de EDI-server eruit als weergegeven in figuur 1.




*Figuur 1. EDI-server.*

*Verklaring van de termen:*

| | |
|---|---|
| Appl. | Applicaties, ongeacht mainframe |
| DMQ | DEC Message Queue (communicatie tussen applicaties) |
| Tracking | Afgifte van tracking nummers en vastleggen van status |
| History | Archiveren van berichten, interchanges, inhuis-bestanden |
| Comm. proc. | Communicatie Proces (afhankelijk van gewenste verbinding) |
| OAPI | Outbound Application Program Interface |
| IAPI | Inbound Application Program Interface |
| OMTR | Outbound Message TRanslator |
| IMTR | Inbound Message TRanslator |
| MIB | Message Interchange Builder |
| ISP | Interchange SPlitter |
| OGWI | Outbound GateWay Interface |
| IGWI | Inbound GateWay Interface |

Het principe is dat een applicatie een te verzenden bericht aan de EDI-server aanbiedt, die daarna de verdere afhandeling volledig zelfstandig uitvoert. Na goede ontvangst van het inhuis-bestand door de EDI-server kan de applicatie het bericht als verzonden beschouwen.

**Inkomend bericht**

*Communicatie Proces*
Het Communicatie Proces (Comm. proc. of CP) is altijd actief en neemt het door de partner aan ECT gestuurde EDIFACT-bericht in ontvangst. Het CP handelt alle specifieke zaken betreffende de communicatie af. Het gaat hier om "protocol" en "dialoog" met het externe systeem, waarbij het onder andere afhankelijk is van de partner op welke wijze de datacommunicatie plaatsvindt. Het protocol zorgt hier voor een betrouwbare, foutloze overdracht van de berichten, waarbij de protocols (software) op beide computersystemen met elkaar "onderhandelen" over de transmissie en, bij storingen, hertransmissie van delen van het bericht. Bij de dialoog gaat het om inlogprocedures (username/password) en commando's voor het opstarten van datacommunicatiesessies.

In principe neemt dit CP altijd het initiatief tot de communicatie. Het "inbellen" vanuit een extern systeem in de EDI-server wordt dan onmogelijk gemaakt, zodat inbrekers ("hackers") geen kans krijgen. In dit verband ligt het dus voor de hand gebruik te maken van een Value Added Network (VAN), zodat beide partners het initiatief moeten nemen tot het leggen van de verbinding, waardoor de beveiliging optimaal is geregeld.

Het CP haalt één of meer bestanden op uit het externe computersysteem (van de partner of VAN), maar "kijkt" niet naar de inhoud of vorm. Een opgehaald bestand wordt na correcte ontvangst op disk gezet en de gegevens over het bestand worden aan de EDI-server doorgegeven. Elk bestand kan één of meer berichten bevatten. Dit wordt later vastgesteld door de "splitter". In deze beschrijving noemen we een dergelijk bestand een "interchange". Een interchange bevat dus één of meer berichten (messages).

*Inbound Gateway Interface*
Zodra het CP een interchange aanbiedt vraagt de Inbound GateWay Interface (IGWI) bij het Tracking Proces een Interchange Tracking Number op en maakt daarmee een Interchange Track-record aan in de Tracking Table van de EDI-server database. Op dit moment is de ontvangen interchange bekend onder het Interchange Tracking Number in de EDI-server.

De IGWI zal nu de interchange aanbieden aan de Interchange SPlitter (ISP) en de Tracking Table wordt bijgewerkt.

*Interchange Splitter*
De ISP splitst de ontvangen interchange in messages. Met andere woorden, de "verzamel-envelop" wordt verwijderd en er zullen één of meer enveloppen met berichten (messages) te voorschijn komen. De ISP vraagt nu per bericht een Message Tracking Number op en maakt daarmee tevens een

Message Track-record aan in de Tracking Table van de EDI-server database.

De interchange wordt door de ISP aan het History Proces aangeboden, waarmee de ontvangen interchange, in de vorm zoals deze is ontvangen, in het archief wordt geplaatst (in de history-directory van de EDI-server).

*De EDI-server heeft tot doel de diverse systemen op eenduidige wijze te voorzien van professionele EDI-faciliteiten.*

De ISP draagt elk afzonderlijk bericht (door middel van het Message Tracking Number) over aan de Inbound Message TRanslator. Tevens wordt de Tracking Table bijgewerkt.

*Inbound Message Translator*
De IMTR haalt aan de hand van de "envelopgegevens" (onder andere partner en berichttype) de gegevens betreffende het berichttype op in de Route Table van de EDI-server database. De Route Table van de EDI-server bevat een aantal vaste gegevens, zoals berichttype, applicatienaam, naam van de partner, naam van de berichtdefinitie en nog een aantal relevante gegevens.

Op dit moment wordt vastgesteld of de desbetreffende afzender inderdaad gerechtigd is het desbetreffende berichttype aan de interne applicatie aan te bieden. Is dat eventueel niet het geval dan zal de EDI-server een foutmelding geven, waarna maatregelen kunnen worden genomen. Het bericht wordt dan in een aparte error-directory geplaatst en niet verder verwerkt.

Aan de hand van de gegevens in de Route Table in de EDI-server database wordt de juiste berichtdefinitie opgehaald. De berichtdefinitie is een met een editor aan te maken en te bewerken bestand, waarin onder andere de volgende gegevens staan:
- berichtstructuur (meestal EDIFACT);
- bijbehorende record-structuur IHF (InHouse File);
- mapping van externe structuur naar IHF;
- code-conversietabellen.

Aan de hand van de berichtdefinitie wordt nu het externe bericht vertaald naar een IHF.

De IHF wordt vervolgens aangeboden aan de Inbound Application Program Interface (IAPI) en de Tracking Table wordt bijgewerkt.

*Inbound Application Program Interface*
De IAPI zal nu de IHF, samen met een aantal routeringsparameters, zoals berichttype en naam van de partner (uit de Route Table), aan de applicatie overdragen.

Zodra de applicatie de goede ontvangst van de IHF heeft bevestigd, zal de IAPI het History Proces opdracht geven de IHF te archiveren. Tevens wordt de Tracking Table bijgewerkt.

**Uitgaand bericht**

*Outbound Application Program Interface*
De applicatie biedt een te verzenden bericht aan, in de vorm van een IHF met parameters, aan de Outbound Application Program Interface (OAPI). Aan de hand van de parameters, zoals geadresseerde en berichttype, zal het desbetreffende record in de Route Table van de EDI-server worden opgehaald. Er wordt een Message Tracking Number opgevraagd aan het Tracking Proces, waarna er een Track-record wordt aangemaakt in de Tracking Table. De IHF wordt klaargezet voor archivering. De OAPI zal het te verzenden bericht vervolgens aanbieden aan de Outbound Message TRanslator (OMTR).

*Outbound Message TRanslator*
De OMTR haalt aan de hand van de gegevens uit de Route Table de desbetreffende berichtdefinitie op en vertaalt de IHF in de juiste EDIFACT-structuur. Hierbij wordt er alleen een binnenenvelop om het bericht gedaan. Na correcte vertaling wordt het EDIFACT-bericht aangeboden aan de Message Interchange Builder (MIB) en wordt het Message Track-record bijgewerkt.

*Message Interchange Builder*
De MIB is het tegenovergestelde van de ISP voor de inkomende berichten. De MIB voegt afzonderlijke berichten voor dezelfde ontvanger samen tot één interchange, indien dit tenminste is toegestaan. Hierover kunnen met de verschillende partners overigens ook verschillende afspraken worden gemaakt.

De MIB kan de berichten zonder vertraging doorgeven. De MIB kan echter zo worden ingesteld dat een interchange pas na een bepaalde tijd wordt geformeerd. Ook is het mogelijk het aantal berichten per interchange te limiteren.

Na het samenstellen van een interchange wordt deze aan de Outbound GateWay Interface (OGWI) ter verzending aangeboden.

*Outbound GateWay Interface*
De OGWI zorgt ervoor dat met behulp van het juiste CP (Communicatie Proces) het te verzenden bericht op correcte wijze naar de ontvanger wordt verzonden.

**Historische gegevens**

Na overdracht van ontvangen berichten aan de applicatie en na overdracht van een te verzenden bericht aan het Communicatie Proces, zullen de Track-records van de EDI-server database worden

overgeheveld naar de historische EDI-server database, te zamen met eventuele vast te leggen inhoudelijke gegevens.

### Recovery

Zolang de gegevens betreffende berichten zich nog in de Tracking Table van de EDI-server bevinden zal recovery van berichten automatisch kunnen plaatsvinden. Bij een eventuele halt van het systeem zal de EDI-server na het opnieuw opstarten van het systeem, geheel automatisch het Recovery Proces (RP) opstarten. Dit RP zal het bericht aan de hand van de status van het bericht, zoals vastgelegd in de Tracking Table van de EDI-server database, wederom aanbieden aan het proces dat zijn taak niet heeft kunnen afmaken. Op deze wijze is het praktisch onmogelijk dat berichten niet naar de applicatie worden doorgegeven, dan wel niet naar de partner worden verzonden. Ook het eventueel dubbel aanbieden van berichten wordt hiermee voorkomen. Het RP is onderdeel van de EDI-server.

### Foutmeldingen

Indien de EDI-server tijdens het verwerken van inkomende en/of uitgaande berichten een fout constateert, waardoor het bericht niet verder kan worden verwerkt, wordt hiervan melding gemaakt aan de systeembeheerder door middel van een bericht in zijn mailbox op het computersysteem. Tevens wordt er een bericht met dezelfde gegevens aan de applicatie verzonden, zodat ook de gebruiker op de hoogte is van het probleem.

In principe mogen er geen fouten optreden, maar als er bijvoorbeeld toch verkeerde codes worden gebruikt of andere, nog niet ontdekte fouten zitten in de applicaties (bij ECT of bij de partner), dan zal de EDI-server, afhankelijk van het soort fout, een waarschuwing of een foutmelding sturen naar de systeembeheerder.

Bij een waarschuwing worden de vertaling en verdere verwerking wel uitgevoerd. Bij een foutmelding zal verdere verwerking niet mogelijk zijn en blijven de gegevens betreffende het bericht in de EDI-server voor inspectie aanwezig.

### User Interface

Na het initieel installeren en configureren van de EDI-server, waarbij onder andere de EDI-berichten worden gedefinieerd en de Route Table wordt gevuld, zal deze in principe zonder gebruikersinterventie kunnen werken. De gebruiker merkt niets van de werking van de EDI-server en er is dan ook geen behoefte aan een uitgebreide User Interface. Zo bezien functioneert de EDI-server als een black box.

## TAAK EN FUNCTIES VAN DE SYSTEEMBEHEERDER

De systeembeheerder kan de volgende zaken op de EDI-server uitvoeren en/of beheren:

### Route-records

De route-records bevinden zich in een database-tabel en moeten eenmalig per combinatie van berichttype/zender/ontvanger worden aangemaakt.

### Berichtdefinities

Berichtdefinities worden per berichttype aangemaakt.

### Foutmelding ontvangen

Zodra de EDI-server op enig moment vaststelt dat, in verband met een fout, een bericht niet verder kan worden afgehandeld, dan wordt er een kort bericht in de mailbox van de systeembeheerder gedeponeerd. Deze krijgt een signaal op zijn terminal en kan dan door het mailbericht te lezen vaststellen waar de fout zich heeft voorgedaan en wat de aard van de fout is. Verdere details van het probleem worden in de logfile aangetroffen, waar ook de inhoud van het EDI-bericht, zoals dit werd ontvangen, kan worden bekeken en/of afgedrukt.

### Logfiles raadplegen

De systeembeheerder zal zo nu en dan de logfiles willen raadplegen. Er is een algemene logfile, waarin alle acties binnen de EDI-server op volgorde van tijd worden vastgelegd, en er is een logfile per bericht, waarin de specifieke handelingen met dat bericht worden geregistreerd. De logfiles kunnen worden gelezen en eventueel worden afgedrukt. Ook detailinformatie betreffende fouten en waarschuwingen worden in de logfile vastgelegd. Nadere gegevens betreffende individuele berichten kunnen in de logfile van het desbetreffende bericht zelf worden aangetroffen. De inhoud van het bericht, zoals dit werd ontvangen of verzonden, kan hier door de systeembeheerder worden bekeken en/of afgedrukt.

### Tracking Tables raadplegen en/of wijzigen

De systeembeheerder kan in de Tracking Table vaststellen wat de status van een bericht is. Ook is het mogelijk de status van een bericht te wijzigen, waardoor een bepaalde stap nog eens kan worden uitgevoerd. Dit is van belang als er iets fout is gegaan, bijvoorbeeld tijdens de vertaling. Als de fout wellicht eenvoudig te herstellen is door het bericht of de inhouse-file aan te passen, dan kan het bericht op deze wijze wederom aan de vertaler worden aangeboden, waarna de volgende stappen eveneens zullen worden uitgevoerd.

## MAATREGELEN

Hieronder volgt een kort overzicht van de maatregelen die getroffen zijn dan wel getroffen zullen worden om de beheersbaarheid van het EDI-verkeer mogelijk te maken. Hierbij speelt bij ECT de EDI-server een belangrijke rol, maar ook de ontwikkelaars van de applicatie-software hebben aandacht voor dit onderwerp.

### Continuïteit

De ECT EDI-server draait op dubbele DEC/VAX-minicomputers, waarbij bij uitval van één van de processoren, de overblijvende processor blijft doorwerken. Ook datacommunicatievoorzieningen zijn dubbel uitgevoerd. In praktisch alle gevallen is het mogelijk door te werken. In het ergste geval zal er moeten worden omgeschakeld en dan zal het EDI-verkeer naar verwachting hooguit vijftien minuten stil komen te liggen. In dat geval treden er voor bepaalde processen met een hoge prioriteit, zoals afhandeling van aan- en afleveringen via de weg, eventueel handmatige procedures in werking. Deze procedures zijn gedetailleerd uitgewerkt en vastgelegd.

### Betrouwbaarheid computersysteem

De EDI-server bewaakt de kwaliteit van het EDI-verkeer, maar niet de inhoud van de berichten. In principe is het mogelijk foutieve gegevens door te geven, mits dit op een geldige manier plaatsvindt. Zo zullen foutieve containernummers in een EDI-bericht door de EDI-server zonder mankeren worden doorgegeven naar de partner of naar de inhuis-applicatie. De inhuis-applicatie zelf zorgt er dus voor dat er geen foutieve containernummers worden aangeboden of verwerkt. Ook het computersysteem van de partner zal ervoor moeten zorgen dat foutieve gegevens niet worden verwerkt of aangeboden.

*Toepassing van een elektronische handtekening in een EDI-bericht maakt controle op bevoegdheden mogelijk.*

De ECT EDI-server zal een transmissie pas als geslaagd melden als zekerheid is verkregen over de correcte en foutloze overdracht van het bericht. Dit betekent dat de transmissie in alle gevallen onder besturing van een protocol zal moeten plaatsvinden. Dit protocol zorgt voor bevestiging van goede ontvangst en hertransmissie van onderdelen van het bericht, als er fouten zijn geconstateerd. Het CP (Communicatie Proces) zal de status in de Tracking Table (audit trail) als "verzonden" melden, als bevestiging is verkregen van het protocol op de externe computer dat het bericht goed is overgedragen. Andersom zal de status "ontvangen" pas worden gemeld, als het bericht correct is ontvangen.

### Vertrouwelijkheid

De ECT EDI-server zorgt ervoor dat bepaalde berichttypen niet aan bepaalde partners kunnen worden verzonden. Andersom geldt ook dat bepaalde partners wel of niet bevoegd zijn bepaalde berichttypen aan te bieden. De EDI-server controleert dit en zal afgekeurde berichten niet verder verwerken. De systeembeheerder krijgt hiervan uiteraard een melding en zal in overleg met de bedrijfsleiding gepaste maatregelen treffen.

Eventuele toepassing van een elektronische handtekening in een EDI-bericht maakt controle op bevoegdheden mogelijk. Dit wordt door de EDI-server als een inhoudelijke zaak beschouwd, waarvoor de applicatie de verantwoordelijkheid draagt. Een elektronische handtekening zal bij toepassing daarvan als een gewoon gegevenselement aan de applicatie worden doorgegeven, dan wel aan de partner. Controle op deze elektronische handtekening is dus de verantwoording van de applicatie intern en de applicatie van de partner.

Door toepassing van hoogwaardige technieken kan de EDI-server zorgen voor codering en decodering van EDI-berichten. Op deze wijze kan dit soort diensten centraal worden verzorgd, zodat alle applicaties en systemen van ECT kunnen profiteren van deze geavanceerde mogelijkheden.

### Bewijsvoering

Zoals eerder beschreven verzorgt de ECT EDI-server het archiveren van EDI-berichten. Berichten worden per dag gearchiveerd en op tape of een ander medium weggeschreven. In deze procedure zijn tevens voorzieningen opgenomen voor het regelmatig verversen van de tapes of andere media. Er zijn uiteraard ook voorzieningen voor het opzoeken en terugladen van individuele berichten.

## TOT SLOT

Bij het geautomatiseerde zenden en ontvangen van grote hoeveelheden EDI-berichten kan er van alles fout gaan en kunnen de problemen al ontstaan bij de berichtontwikkeling, nog voordat er sprake is van enig gebruik.

Het is daarom van groot belang reeds in de fase van het ontwikkelen van berichten deel te nemen, zodat invloed kan worden uitgeoefend op berichtsoorten, structuur en inhoud. Standaardberichten (UN/EDIFACT) worden meestal door verschillende bedrijven en instellingen van een bedrijfstak of -kolom ontwikkeld. Hiertoe wordt dan een projectgroep geformeerd, bestaande uit eindgebruikers, EDP- en EDI-specialisten, al of niet onder de para-

plu van een speciaal voor dit doel opgerichte organisatie.

Vast staat in ieder geval dat deelname aan een dergelijke groep de mogelijkheid geeft invloed uit te oefenen op de ontwikkeling van de berichten, zodat de wensen op het gebied van beveiliging en beheersing kunnen worden ingebracht.

De Rotterdamse havenbedrijven hebben met dit doel voor ogen Intis opgericht. Intis zet zich in voor de ontwikkeling van standaard-UN/EDIFACT-berichten in het kader van het EDI-verkeer met de Rotterdamse havenbedrijven. Hiertoe worden projecten geselecteerd, waarvoor door project- en werkgroepen berichten worden geïdentificeerd en daarna ontworpen. De leden van de project- en/of werkgroepen zijn onder andere afkomstig van verschillende havenbedrijven, maar ook exporteurs en importeurs hebben inbreng. Zo worden er in de Rotterdamse haven standaard-UN/EDIFACT-berichten ontworpen en ingediend bij de EDIFACT Board. De aldus ontworpen berichten worden op deze wijze wereldstandaard.

Er zijn ook andere groepen actief, waaronder de SMDG, Shipplanning Message Development Group, een door de EDIFACT Board als zodanig erkende Pan European Group. Deze internationale groep houdt zich bezig met de ontwikkeling van UN/EDIFACT-berichten in het kader van de scheepsplanning, zoals stuwplannen en stuwage-instructies.

Door deel te nemen in de project- en/of werkgroepen van Intis, alsmede in de SMDG, heeft ECT invloed op het ontwerp van de berichten. Op deze wijze kan ECT haar wensen realiseren, uiteraard geheel in overleg en afstemming met de andere deelnemers. Niet-deelnemers kunnen echter slechts in beperkte mate hun ideeën kwijt, terwijl zij vaak door gebrek aan kennis en ervaring op dit gebied het resultaat niet goed kunnen beoordelen.

## SAMENVATTING

Beginnen met EDI is niet zo moeilijk. De complexiteit neemt echter snel toe zodra er meerdere verschillende berichttypen met meerdere partners moeten worden uitgewisseld. Op dat moment kan de beheersbaarheid een probleem worden.

De mogelijke risico's hebben betrekking op de volgende onderwerpen:
1. continuïteit;
2. betrouwbaarheid intern computersysteem;
3. vertrouwelijkheid;
4. bewijsvoering.

Teneinde deze gevaren het hoofd te kunnen bieden, moet er een aantal maatregelen worden genomen, zoals voorzieningen in de apparatuur en programmatuur, maar ook moeten er afspraken worden gemaakt en procedures worden vastgelegd. Ten slotte wordt het bedrijf bij het toepassen van EDI steeds afhankelijker van de techniek, terwijl de beheersing van de specifieke problemen, risico's en gevaren die te maken hebben met deze nieuwe manier van communiceren, ook een specifieke aanpak vereisen.

Dit artikel geeft enig inzicht in deze materie en probeert duidelijk te maken van welke kant de gevaren zijn te verwachten en op welke wijze deze gevaren kunnen worden beheerst. Bij het elimineren van risico's dient de vraag te worden gesteld of nog een praktisch werkbare situatie blijft bestaan. Ook hier is het van belang de gulden middenweg te vinden, waardoor efficiënt en verantwoord EDI-verkeer mogelijk wordt tegen aanvaardbare kosten en acceptabele risico's.

## LITERATUUR

[EDI91] *EDI in de Handel*, Samsom, 1991.

[Hofm89] W.J. Hofman, *EDI Handboek*, Tutein Nolthenius, 1989.

[EDIC90] EDICA, *EDI Control Guide*, EDI Council of Australia and the EDP Auditors Association, 1990.

*G.J. Endenburg RI*
*Is werkzaam bij Europe Combined Terminals BV te Rotterdam als EDI-consultant van de afdeling Informatie Systemen.*
*Hij werkt sinds 1963 in de Rotterdamse haven en houdt zich sinds 1979 bezig met het automatiseren van scheepvaart- en havenbedrijven.*
*In zijn functie van EDI-consultant bij ECT is hij verantwoordelijk voor de ontwikkeling van voorzieningen welke EDI mogelijk maken.*

# EDI bij de Rijksdienst voor het Wegverkeer

J.W.J. Laan

**De meeste Nederlanders van achttien jaar en ouder hebben een relatie met de Rijksdienst voor het Wegverkeer.
In deze situatie worden hoge eisen gesteld aan de betrouwbaarheid van de geautomatiseerde toepassingen, waaronder EDI.
Maar daarnaast zijn andere kwaliteitsaspecten van groot belang.
Laan beschrijft de gevolgen van EDI bij een "producent" van informatie vooral met betrekking tot de performance
en de continuïteit.**

## INLEIDING

De Rijksdienst voor het Wegverkeer (RDW) is een fabriek met als grondstof informatie en als uitvoerprodukt informatie. En die informatie is nogal divers. Want de RDW is niet alleen een bereider van kentekeninformatie en dergelijke, maar ook een voorbereider van wetgeving. Wetten waardoor niet alleen de burger maar ook de RDW zelf gereguleerd wordt. Het meest echter is de RDW bekend van het Deel-III, de kentekendatabase, de APK-keuring, de toelating van voertuigen op de weg en het Centraal Register Rijbewijzen (CRR).

De RDW wordt vaak genoemd in de "Big Brother is watching You"-verhalen. En inderdaad, de RDW heeft een relatie met de meeste Nederlanders van achttien jaar en ouder. Een situatie waarin het maken van fouten tot veel ophef kan leiden.

Dit alles stelt hoge eisen aan de kwaliteit van deze rijksdienst. Uit de brede reeks van aspecten die bij het streven naar deze kwaliteit een rol spelen wordt er hier één uitgelicht: EDI en de manier waarop het zich bij de RDW ontwikkeld heeft in vijftien jaar. De hier gekozen invalshoek op EDI is een technische en behandelt de volgende voor de RDW belangrijke onderwerpen:

- performance, omdat er een groot aantal interactieve, tijdkritische toepassingen is;
- beschikbaarheid, omdat de maatschappij steeds afhankelijker is geworden van de online-gegevensverwerking bij de RDW;
- autorisatie, omdat de RDW een groot aantal zeer verschillende gebruikers heeft en de overheid een grote verantwoordelijkheid heeft voor de privacy- en fraude-aspecten van haar informatiesystemen;
- standaardisatie, omdat de RDW snel moet kunnen inspelen op nieuwe toepassingen voor nieuwe gebruikers.

## EDI BIJ DE RDW

Voor bedrijven die zoeken naar de baten van EDI kan de besluitvorming binnen de RDW vermoedelijk niet als voorbeeld dienen, omdat de uitgangspunten van de meeste bedrijven anders zijn dan die van een rijksdienst. In dit verband zijn twee verschillen te noemen:

1. De RDW is verplicht - bij wet geregeld - informatie te verstrekken aan diverse overheidsinstanties als justitie, politie, defensie en Centraal Bureau Motorrijtuigen (CBM). De combinatie van factoren als snelheid, grote hoeveelheden, continuïteit en integriteit maakt EDI zeer voor de hand liggend.

2. In een kosten/baten-overweging van de rijksdienst zal winst maken nooit een rol spelen, maar wel kwaliteit en efficiëntie.

Bij de RDW heeft EDI geleid tot een verbetering van kwaliteit en efficiëntie. Daarnaast biedt EDI de mogelijkheden om te komen tot de vereiste snelheid, beschikbaarheid en integriteit van informatieverstrekking.
De tabel hiernaast geeft een beeld van de huidige omvang van de geautomatiseerde gegevensverwerking bij de RDW.

| | | |
|---|---|---|
| Gebruikers | ± 20.000, bijvoorbeeld alle Nederlandse gemeenten ten behoeve van rijbewijzen, bijna alle garagebedrijven voor APK, de politiebureaus. | |
| Datacommunicatie Huurlijnen | ± 100, waarachter weer diverse netwerken, zoals die van de PTT, de politie, de verzekeringswereld en de autobranche. | |
| Datanet-1-aansluitingen | ± 200 | |
| Viditel-aansluitingen | ± 250 (maximaal tegelijkertijd) | |
| RDW-terminals | ± 650 | |
| 'Landelijke' databases | Kenteken: | ± 8.000.000 voertuigen + eigenaren |
| | APK: | ± 4.500.000 keuringen |
| | CRWAM: | ± 26.000.000 registraties inclusief historie |
| | CRR: | ± 8.500.000 rijbewijzen + houders |
| Transacties per dag | ± 250.000 | |
| Transactiepiek | 30 transacties per seconde | |

*Tabel 1. Huidige omvang geautomatiseerde gegevensverwerking bij de RDW.*

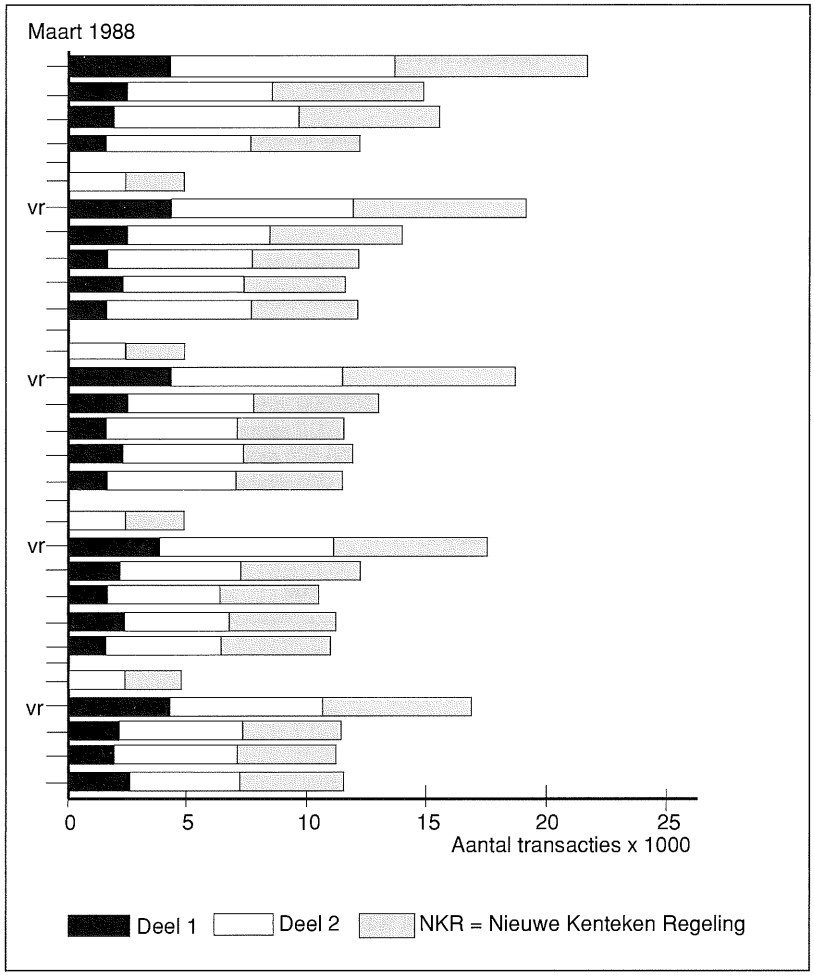
De mutatiestromen van APK en CRR lopen volledig via online-verwerking. De Centrale Registratie Kentekens (CRK) verkeert in een overgangsfase van batch- naar online-verwerking. En de mutaties ten behoeve van de Centrale Registratie Wettelijke Aansprakelijkheid Motorrijtuigen (CRWAM) komen nu nog binnen op tapes en worden batch-gewijs verwerkt, maar binnenkort zullen daarvoor X.400 en EDIFACT worden ingezet.

## PERFORMANCE

De performance van de interactieve gegevensuitwisseling heeft altijd grote aandacht van de afdeling Automatisering van de RDW gehad. Dit was niet altijd een vereiste van iedere gebruiker. Voor de grote hoeveelheid van data-invoer van de RDW zelf moest men snelle responstijden hebben. Nu werd in de tweede helft van de jaren zeventig de meeste software door de RDW zelf ontwikkeld. En als men iets werkends had, werd dat zoveel mogelijk opnieuw gebruikt voor een volgende toepassing. Het aantal gebruikers groeide gestaag. En deze nieuwe afnemers werden op dezelfde manier aangesloten met dezelfde prioriteit en ze werden met dezelfde techniek binnen het systeem afgehandeld, simpelweg omdat de tools om het anders te doen ontbraken.

Het moge duidelijk zijn dat waar men zo'n groot aantal transacties per dag verwerkt, er gelet wordt op een efficiënt transactieverloop, maar de accenten zijn verschoven. In het verleden werd er zeer veel tijd gestoken in het streven dat de transacties een zo gering mogelijk CPU-gebruik hadden met zo weinig mogelijk input- en output-acties op schijf (IO's). Ook besteedde men veel aandacht aan een zo compact mogelijk bericht om de datacomlijnen zo weinig mogelijk te belasten. Het resultaat was een transactieprogramma met de veelzeggende naam High-Speed-Link (HSL). Het was dan ook geschreven in assembler evenals het database management-systeem dat FAM heette (File Access Manager). Om de lengte van berichten minimaal te krijgen waren alle spaties aan het einde van een rubriek uit de berichten gehaald. De rubrieken werden gescheiden door "hekjes" (#). Deze HSL, bestaande uit enkele tienduizenden in assembler geschreven statements, regelde zowel de polling van de DC-lijnen, de toegang op de kentekendatabase als de opmaak en afhandeling van het bericht. De responstijd van de HSL - gemiddeld tussen de honderd en driehonderd milliseconden interne procestijd - was fantastisch, maar de kleinste wijziging in het programma was ten eerste voorbehouden aan mensen die "more than a bit" van bitten afwisten en ten tweede vergde zo'n programmawijziging erg veel tijd.

De flexibiliteit van de toenmalige HSL had veel weg van een blok beton. In 1983 is daarom de HSL zowel in software als bijbehorende hardware in lagen opgesplitst. De toenmalige hardware werd uitgebreid met een datacommunicatie front-end-processor (DCP). Deze geeft invulling aan de eerste drie lagen van het OSI-referentiemodel (X.25). Daarmee deed de eerste standaardisatie op het gebied van datacommunicatie haar intrede. Het overige stuk van de HSL werd opgedeeld in een database-server en per bericht een applicatie-server. Hiermee nam de flexibiliteit enorm toe met betrekking tot de datacommunicatie en de applicaties die de EDI verzorgen.
Het eigen in assembler geschreven database management-systeem FAM bleek veel moeilijker te




*Figuur 1. Dagelijkse overschrijvingen kentekens maart 1988.*

vervangen en bleef derhalve nog een blok aan het been. Het heeft dan ook nog bijna tien jaar geduurd totdat FAM ten grave gedragen werd en werd vervangen door een Relationeel Database Management Systeem (RDMS). RDMS gebruikt echter tien keer zoveel CPU als FAM en doet twee keer zoveel IO's. Desondanks is de interne procestijd niet of nauwelijks langer dan in 1983, doordat ook de capaciteit van de huidige hardware is toegenomen.

De performance van een systeem is in principe recht evenredig met de kracht van de hardware en omgekeerd evenredig met de belasting van de applicatie. Dit gaat op zolang er in het systeem geen bottleneck met betrekking tot CPU-, memory- of IO-capaciteit is ontstaan. Bij online-verwerking kan het systeem tijdens de piek uit balance raken. Het laat zich goed vergelijken met de capaciteit van een wegennet. Onze grote vierbaanswegen kunnen met gemak enkele miljoenen auto's per dag aan. Een probleem echter vormen de ochtend- en de avondspits. Dit kan opstoppingen geven met als gevolg dat er tijdens de spits een kleiner aantal verwerkt wordt dan op minder drukke momenten, terwijl de behoefte groter is.
Transactiequeues zijn net verkeersfiles. Indien men zich over te verwachten queues geen goed beeld kan vormen voordat een nieuwe toepassing in produktie gaat (en men moet aantallen verwerken als bij de RDW), dan kan dat leiden tot onzekerheid. Indien het mogelijk is de load gefaseerd op te voeren, door bijvoorbeeld het aantal gebruikers beetje bij beetje uit te breiden, kan men de greep op de performance wellicht blijven houden. Is men echter verplicht tot een invoering ineens - bij een rijksdienst is dat gebruikelijk op het moment van de inwerkingtreding van de wet - dan kan dat tot catastrofes leiden met betrekking tot de responstijden.

Hoe kan men zich een beeld vormen van de load van een nieuwe applicatie? Dit is te verduidelijken met een RDW-praktijkvoorbeeld.

Op een zeker moment wilde de minister van Verkeer en Waterstaat drs. N. Smit-Kroes iets doen aan bestrijding van fraude met auto's en kentekens. Daarvoor, vond zij, was een Nieuwe Kenteken Regeling (NKR) nodig, waarin onder meer geregeld zou moeten worden, dat voordat een auto verkocht mocht worden:

a. aan alle verplichtingen zoals APK, wegenbelasting en WAM voldaan moest zijn;
b. het onder a. genoemde online gecontroleerd moest worden op het postkantoor;
c. zowel de oude als de nieuwe eigenaar zich met een geldig legitimatiebewijs bij een loket moest vervoegen om deze overschrijving online te laten uitvoeren.

De oude procedure vereist slechts dat iemand (meestal een autohandelaar) de papieren op een postkantoor in orde maakt. De nieuwe procedure zou moeten gelden voor een overschrijving op een nieuwe eigenaar, het in handelsvoorraad nemen, maar ook voor sloop, kortom voor alle wijzigingen van aansprakelijkheid betreffende dat voertuig.

Voor de bepaling van de mogelijke systeembelasting/capaciteit moeten bekend zijn:

1. de frequentie van de transacties met de transactiepiek;
2. de gemiddelde machinebelasting van iedere individuele transactie, het zogenaamde transactieprofiel.

Gemiddeld zou deze nieuwe regeling zo'n 14.000 overschrijvingen per dag gaan opleveren, hetgeen neerkomt op 1,5 transactie per seconde. Uit het kentekenregister echter is een grafiek samengesteld met daarop het aantal overschrijvingen van voertuigen per dag (zie figuur 1). De grafiek bevat drie elementen:

1. de datum deel-I geeft aan wanneer het voertuig voor het eerst op de weg kwam;
2. de datum deel-II geeft aan wanneer het voertuig voor het laatst tenaamgesteld is. Is de datum deel-I gelijk aan datum deel-II, dan betreft het een eerste tenaamstelling;
3. bij NKR worden de huidige vrijwaringen door autohandelaren vervangen door overschrijvingen. De prognose voor NKR is hierop gebaseerd.

Uit de grafiek blijkt dat de topdrukte vrijdags is. Dan bedraagt het aantal circa 20.000. In december

daalt de tenaamstelling van nieuwe auto's tot nul. De reden daarvoor is, dat men in de autohandel de datum deel-I als bouwjaar is gaan beschouwen. Door enkele dagen te wachten met de eerste tenaamstelling bereikt men dat een auto een nieuw "bouwjaar" krijgt. Op de eerste werkdag van januari moet een stuwmeer van overschrijvingen door de PTT-loketten worden verwerkt. Dan wisselen zo'n 32.500 auto's van eigenaar. Dat is bijna 2,5 keer zoveel als het aanvankelijk berekende gemiddelde per dag.
Uit een grafiek van de PTT-loketactiviteiten blijkt dat de toeloop op de loketten tijdens de dagpiek 2,5 keer zo hoog is als het daggemiddelde (zie figuur 2).
Hieruit is te concluderen dat op 2 januari tijdens de piek niet de verwachte 1,5 transactie per seconde van deze online-toepassing zal komen, maar ruim 9 transacties per seconde.

Dit alles was aan de hand van beschikbare gegevens te herleiden. Maar er zit nog een addertje onder het gras. Namelijk het feit dat niet een autohandelaar in zijn eentje naar het postkantoor moet komen om de papieren in orde te maken, maar dat tegelijkertijd de oude en de nieuwe eigenaar zich aan het loket dienen te vervoegen. Dit kan aan het huidige geconstateerde piekgedrag aan het loket wel eens een vreemde wending geven. In plaats van om elf uur 's morgens zou de toeloop op de loketten voor deze handelingen wel eens na werktijd kunnen liggen. Immers, wie is er bereid een snipperdag te nemen om een auto over te schrijven? Daarmee wordt de bruikbare lokettijd misschien niet acht uur per dag maar slechts twee à drie uur. Dat zou de piek drie tot vier keer hoger maken.

Dit zijn niet de enige gevolgen van de gecontroleerde online-afgifte. Want wat zijn de consequenties van het feit, dat een overschrijving pas mag plaatsvinden nadat aan alle verplichtingen is voldaan. Ten behoeve van deze controle moet er een online-registratie zijn van het voldaan hebben aan de APK-plicht, het betaald hebben van de wegenbelasting en de aanmelding van de Wettelijke Aansprakelijkheid Motorrijtuigen (WAM).

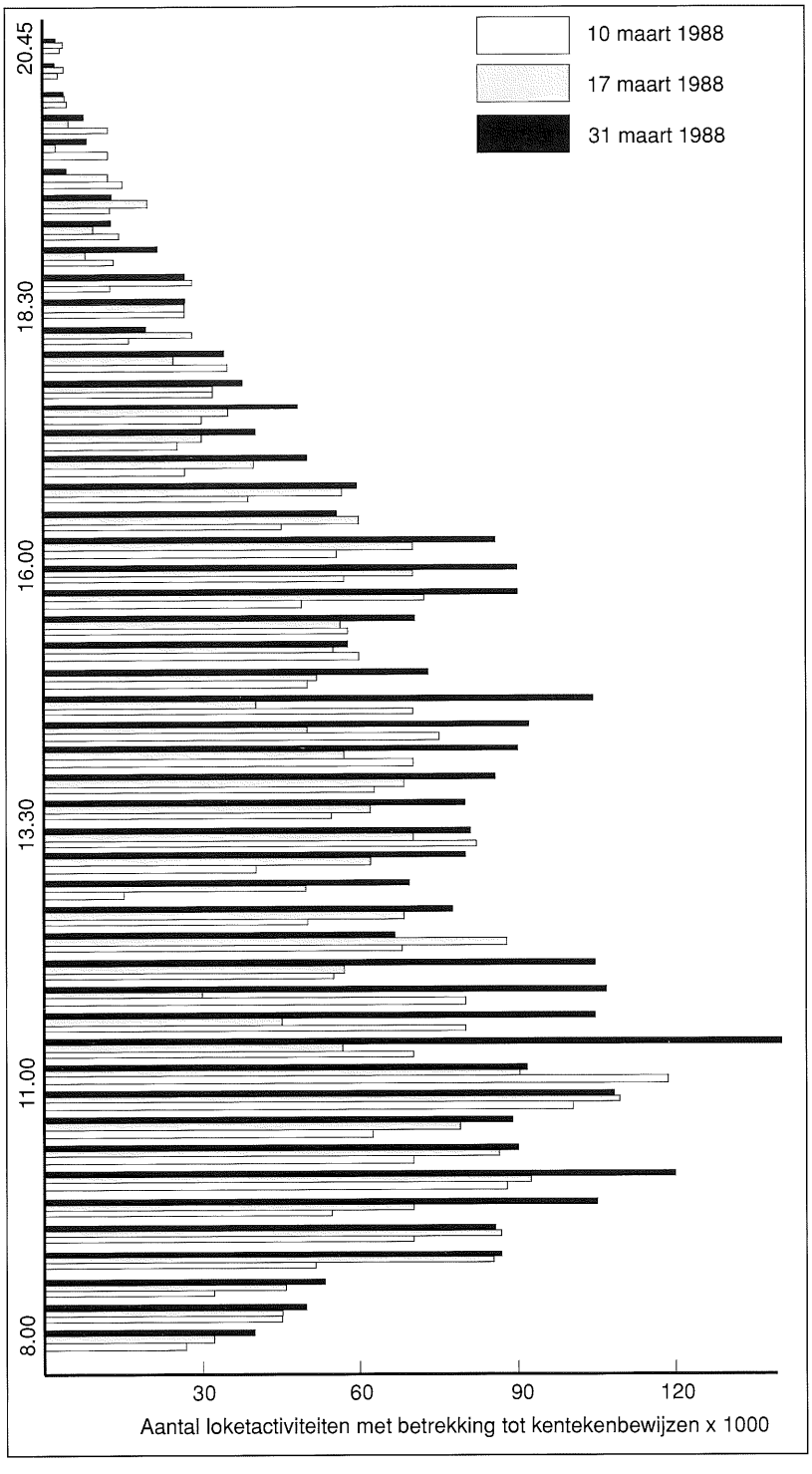
De 4,5 miljoen online-APK-registraties gebeuren nu reeds bij de RDW.

Van de huidige betalingen van de motorrijtuigen- of wegenbelasting vindt geen online-gegevensuitwisseling plaats met het CBM. Indien het RDW-register up-to-date zou moeten zijn voor deze gegevens, vergt dat ongeveer 25 miljoen updates per jaar bij de RDW of een online-verbinding naar het CBM.

De verzekeringsmaatschappijen leveren nu per tape ongeveer 6 miljoen mutaties CRWAM. Vanwege de hoge eisen ten aanzien van actualiteit moeten ook deze mutaties via EDI geschieden.

Om 4 miljoen overschrijvingen online-gecontroleerd te kunnen uitvoeren is het nodig 35 miljoen extra online-updates uit te voeren.

Dit voorstel van Smit-Kroes heeft het niet gehaald. Niet vanwege performance of vanwege de hard-




*Figuur 2. PTT-loketactiviteiten op vrijdag met betrekking tot kentekenbewijzen.*

ware-kosten, maar omdat er geen maatschappelijk draagvlak voor was. De autobranche en de verzekeringswereld konden zich er niet in vinden.

Een nieuwe wet komt er wel. Ook een nieuw informatiesysteem, waarbij EDI een grote rol speelt. En in het implementatietraject van dit systeem is wel degelijk rekening gehouden met de problemen die men heeft bij een plotselinge invoering. Hierdoor

wordt niet alleen het risico gemeden, dat de computer of het netwerk zou kunnen worden opgeblazen, maar ook dat de organisaties van de RDW, het CBM en de PTT onder hoge druk komen te staan; een geleidelijke implementatie verloopt bij instanties als deze immers veel soepeler.

Naast de piek is het gemiddelde load-profiel van een transactie een bepalende factor. Het probleem is vaak dat de applicatie nog moet worden ontwikkeld.

Ter bepaling van de benodigde machinecapaciteit is het zeer gebruikelijk met vuistregels te werken. Een andere methode is een soortgelijke applicatie model te laten staan voor de nieuwe. Bij de RDW is een hulpmiddel gebouwd om de load te berekenen.

*Naarmate de trend zich voortzet dat de applicaties steeds meer gebruik maken van online-verwerking in plaats van batch wordt de afhankelijkheid van het up zijn van een computer steeds groter.*

De RDW heeft zelf een datadictionary ontwikkeld, waarin voorzieningen zijn getroffen om de te verwachten computerbelasting te berekenen. Dit gebeurt op basis van het datamodel en de toegangspadanalyse(s) van de processen (transacties). Aan de hand van deze functionele informatie vastgelegd in de datadictionary en gegevens over procesfrequentie, de manier van verwerking (batch of online) en de machinecapaciteit zoals CPU-power en IO-tijden, wordt een berekening gemaakt van de transactieprofielen. Hierna kan men berekenen de respons- respectievelijk batch-tijden en het maximum haalbare aantal transacties per seconde.

Op deze manier is het mogelijk reeds zeer vroeg vrij exact de impact op het gebied van hardware te voorspellen. Tevens biedt het de mogelijkheid de consequenties van de keuzen die men heeft bij het vaststellen van het technisch datamodel, door te rekenen. Hiermee bereikt men dat men het meest optimale technische datamodel bepaalt bij de gegeven processen.

## BESCHIKBAARHEID

Een wezenlijk deel van de inspanning die het rekencentrum van de RDW zich getroost, komt op rekening van het streven naar een zo hoog mogelijke beschikbaarheid van de informatiesystemen. Naarmate de trend zich voortzet dat de applicaties steeds meer gebruik maken van online-verwerking in plaats van batch wordt de afhankelijkheid van het up zijn van een computer steeds groter. Indien op dit moment de centrale computer van de RDW down is, stagneren de APK-meldingen van de garagebedrijven, de gecontroleerde afgifte van rijbewijzen en voertuigdocumenten, en vooral ook de informatieverstrekking aan politie en justitie. De RDW moet 24 uur per dag beschikbaar zijn gedurende zeven dagen per week.

Dit bleek eens temeer toen in februari 1990 de boeren in Veendam het gebouw van de RDW bezetten. Op de onbemande computer liep een aantal online-processen gewoon door. Dit duurde reeds zo'n veertien dagen, toen het moment was aangebroken van een systeemstop. Op last van het ministerie van Justitie maakte de ME toen binnen enkele uren een eind aan de bezetting; vanaf dat moment werden maatregelen tegen dergelijke calamiteiten bespreekbaar. Maatregelen die de RDW na een risico-analyse al enige tijd op een verlanglijstje had staan.

Al sinds 1975 werden er steeds maatregelen genomen om de zogenaamde "single points of failure" uit te sluiten. In dit kader werden onder meer de volgende maatregelen genomen:

- Het dubbel uitvoeren van diverse hardware-onderdelen, zoals CPU's, controlers, channels, en datacommunicatielijnen en -processoren.

- Het volledig scheiden van ontwikkel- en produktiewerkzaamheden door invoering van een ontwikkelmachine. Hierdoor werd het tevens makkelijker de systeem-software uit te testen.

- De ingebruikneming van een no-break-installatie ten behoeve van de stroomvoorziening.

- De aanschaf van een tape-robot, waardoor er geen operator meer nodig is voor tape-handling, bijvoorbeeld om de log-tapes ten behoeve van database recovery op te hangen. Ook kan men nu onbemand 's nachts de tape-backups van de databases maken. Hierdoor is regelmatig backuppen geen bezwaar.

- Naast het OFR-systeem (Onbemand Functioneren Rekencentrum) het instellen van een 24-uurs bemanning van het rekencentrum inclusief bewakingsdienst. OFR is een zelf ontwikkeld stuk software en hardware, dat controleert of alle vitale onderdelen van het systeem nog functioneren en zo niet, dan wordt een operator opgeroepen, die de eventuele storing moet (laten) verhelpen. Het nadeel van OFR is, dat er enige tijd verloren gaat voordat de dienstdoende operator aanwezig is.

- Het dubbel uitvoeren van alle schijven en deze in duplo up-to-date houden, zodat de uitval van een schijfeenheid geen verstoring geeft in de produktie.

- Ten slotte het inrichten van een compleet uitwijkcentrum.

Het uitwijkcentrum wordt gekenmerkt door de volgende eigenschappen:

– Op het uitwijkcentrum staat een computer, die normaal wordt gebruikt voor ontwikkel- en testwerkzaamheden, maar die voldoende capaciteit heeft om de produktie over te nemen. De omschakeling gebeurt nog handmatig. De consequentie van een eventuele uitwijk is dat de afdeling Systeemontwikkeling het programmeren en testen moet staken, en dat er enig tijdverlies is ten behoeve van de opstart van het standby-systeem.

– De eerder vermelde online-bijgehouden kopieën van de schijven staan op het uitwijkcentrum. Het up-to-date houden gebeurt via glasvezels vanuit de hoofdcomputer. Hierdoor hoeft men bij uitwijk niet eerst de databases op te bouwen.

– De datacommunicatievoorzieningen zijn ten behoeve van uitwijk niet alleen gedupliceerd bij de RDW, maar ook bij de PTT. Oorspronkelijk liepen alle PTT-verbindingen via een knooppunt in Groningen. Nu is er door middel van een straalzender op het terrein van het uitwijkcentrum een alternatieve datacommunicatieverbinding gecreëerd.

Beschikbaarheid heeft evenals performance haar prijs. Deze prijs heeft de neiging exponentieel hoger te worden naarmate men hogere eisen aan de beschikbaarheid of de performance stelt.

Naast deze bovengenoemde preventieve maatregelen, die alle veel investeringen vergen, is er nog een aantal van organisatorische en procedurele aard. Het geheel van deze maatregelen wordt vastgelegd in een kwaliteitssysteem. Het kwaliteitssysteem moet de informatietechnologie binnen de RDW op een hoger plan brengen. En hoewel dit proces zeker niet zonder moeite en kosten gaat, groeit de overtuiging dat naarmate het kwaliteitssysteem verder zal worden uitgebouwd en ingevoerd, het uiteindelijk niet duurder is maar juist kostenbesparend zal zijn. Deze besparingen zullen vooral moeten komen uit de lagere kosten voor curatieve maatregelen.

## AUTORISATIE

Omdat de RDW verscheidene datacommunicatieprotocollen ondersteunt, zijn van oudsher nogal wat verschillende uitvoeringen van autorisatie ontstaan. Zo zijn er aansluitingen aan het telexnetwerk, Viditel, Datanet-1, dial-up en huurlijnen. Bij dit alles verschilt de filosofie achter de autorisatie niet van elders gangbare. Bovendien is autorisatie sterk gebonden aan die welke het operating systeem biedt. Een aparte plaats wordt hier ingenomen door de program-to-program-toepassingen. Bij program-to-program valt de autorisatie van de sessie die de host-computer heeft met de andere host-computer onder de systeem-software. Het operating systeem echter op de ene host kan onmogelijk weten, wie de eindgebruiker op de andere host is. In dit geval kan men de autorisatie op twee manieren regelen:

1. Men delegeert de autorisatie volledig aan de host van het andere rekencentrum. De consequentie is dat men:
   a. een verklaring van een onafhankelijke deskundige moet eisen;
   b. zelf positief moet kunnen aantonen welke transacties van welk rekencentrum komen.

2. Men houdt zelf de autorisatie van en verantwoording aan de eindgebruiker op de andere host in handen. De consequenties hiervan zijn dat:
   a. een verklaring van een onafhankelijke deskundige dat bij dat andere rekencentrum voldoende waarborgen zijn voor een betrouwbare geautomatiseerde gegevensverwerking, nodig blijft;
   b. men nog steeds positief moet aantonen vanwaar de transacties komen;
   c. men ieder binnengekomen bericht moet autoriseren/identificeren. Het is immers anders alleen bekend van welke computer dit bericht komt en niet van welke gebruiker;
   d. men een verantwoording aan de individuele eindgebruiker kan afleggen over alle acties die hij/zij heeft gepleegd.

De meerkosten van de tweede methode zitten in het autoriseren/identificeren per binnengekomen bericht. De meerwaarde komt uit het feit dat men aan iedere individuele gebruiker een verantwoording kan afleggen van wat men voor hem/haar aan berichten heeft verwerkt. Zowel de eerste als de tweede optie is bij de RDW in gebruik en wordt beheerd in een systeem Beheer Bericht Systemen (BBS).

*Bij het nastreven van standaardisatie wordt het als een probleem ervaren dat op een mainframe een standaard veel langer op zich laat wachten dan op een PC en dat men met de invoering ervan alles zeer goed met de betrokken partners dient af te stemmen.*

In BBS zijn de volgende maatregelen geïncorporeerd:
- user-id/password;
- testen op netwerkadressen; een gebruiker kan slechts op één of enkele lijnen binnenkomen;
- encryptie;
- openingstijden; een user-id wordt geweigerd buiten de door de gebruiker zelf gedefinieerde openingstijden;
- vermelden van sleutelgegevens van het vorige bericht, zodat een onderbreking van die ketting of door de autorisatie of door de eindgebruiker kan worden geconstateerd;
- het rapporteren aan gebruiker van de door hem afgenomen diensten.

*J.W.J. Laan*
*Trad in 1981 in dienst van de RDW. Tot 1985 functioneerde hij als systeemingenieur, waarna hij de leiding over de afdeling Onderzoek & Ondersteuning (O&O) op zich kreeg.*
*O&O is een bureau met acht specialisten en geeft advies aan de afdeling Systeem Ontwikkeling op het gebied van datacommunicatiegebruik, data-administratie, database-ontwerp, methoden en technieken (kwaliteitssysteem), en software-pakketten (compilers, 4GL, SQL, etc.).*

## STANDAARDISATIE

Als de RDW ergens aan lijdt is het de "wet van de remmende voorsprong". Indien iets moeizaam tot stand gekomen is - zeker als er meerdere partners bij betrokken zijn -, wordt het nog moeizamer geïnnoveerd.

In 1983 deed X.25 zijn intrede bij de RDW en dit verving het zelf in assembler geschreven protocol. Ten behoeve van het CRR-systeem wordt er sinds 1985 gewerkt met Videotex. Dit wordt ook voor APK veelvuldig gebruikt. Tevens maakte CRR de ondersteuning van 3270 (IBM) noodzakelijk.

Ten behoeve van de presentatie van de berichten is in 1990 BAR (Bericht Afhandeling RDW) ontworpen. BAR is bedoeld voor de bericht-layout van interactieve program-to-program-toepassingen. Het is flexibeler in onderhoud, maar geeft in vergelijking met het oude HSL-protocol een bericht dat minstens drie maal zo lang is.

Sinds 1992 wordt er getest met X.400, FTAM en EDIFACT. Deze produkten zullen in het vierde kwartaal van 1992 in twee pilotprojecten worden ingezet. De produkten X.400 en FTAM zijn van Unisys. Als EDIFACT-vertaler zal EDI*CENTRAL van General Electric worden gebruikt. De pilot-projecten worden gedaan met het Centraal Justitieel Incasso-Bureau ten behoeve van het innen van bekeuringen en met het Assurantie DataNet (ADN) om de WAM-mutaties van de verzekeraars aan te leveren via EDI in plaats van op tape.

Ook heeft er op het gebied van database management-systemen een standaardisatie plaatsgehad. Van 1974 tot 1992 werd voor de kentekenregistratie FAM gebruikt, dat door de RDW zelf geschreven en onderhouden werd. Vanaf 1984 is ten behoeve van CRR een codasyl Database Management System (DMS-IIOO) operationeel. Maar sinds 1990 wordt er bij alle nieuwe ontwikkelingen gebruik gemaakt van een Relational Database Management System (RDMS-IIOO). Hierin gebeuren alle gegevensmanipulaties met Structured Query Language (SQL).

Wilde men in het verleden iets in de bevoegdheden besturen, dan moest dat worden geprogrammeerd. In de loop der tijd echter is het autorisatiepakket van het operating systeem zeer compleet geworden. Zo is te definiëren wat de bevoegdheden van een gebruiker zijn en op welke stukken van de database hij toegang heeft. BBS is ontwikkeld om de bevoegdheden te beheren van een gebruiker die aangelogd is aan een andere host. Hierin voorziet het operating systeem niet.

De problemen waarmee de RDW in de toekomst geconfronteerd wordt, zullen zowel van functioneel-inhoudelijke als van technische aard zijn. Naast een uitbreiding van zijn binnenlandse taken kan het "Europa '92" andere eisen gaan stellen, en dat niet alleen aan de datacommunicatie. Er kan gevraagd worden om internationalisatie van de applicaties, hetgeen inhoudt: diverse charactersets, teksten in meerdere talen, ondersteuning van diakritische tekens (is nu reeds een probleem) en dergelijke.

Hierdoor zijn flexibiliteit en standaardisatie een eerste vereiste bij de ontwikkelingen binnen de RDW. De grote handicap van de RDW is echter dat de massaliteit van gegevensverwerking de RDW weinig flexibel maakt. Grote databases en grote netwerken laten zich nu eenmaal niet snel reorganiseren. Bovendien moeten de eisen van performance gehaald blijven worden.
Bij het nastreven van standaardisatie wordt het als probleem ervaren dat op een mainframe een standaard veel langer op zich laat wachten dan op een PC en dat men met de invoering ervan alles zeer goed met de betrokken partners dient af te stemmen. Een migratie naar standaarden is daardoor een moeizaam proces. Derhalve hebben nieuwe ontwikkelingen in standaarden wel de voortdurende aandacht, maar blijft de implementatie ervan vaak nog achter de horizon liggen.

# EDI, een strategisch perspectief voor het bankwezen

Drs. M.A. Bongers RE en mw. drs. M. Steeman

**In hoeverre zijn banken in staat "to close the loop" inzake EDI? Gaan banken in de toekomst ook een centrale positie in het elektronisch berichtenverkeer innemen of verliezen zij nu reeds terrein op de grote aanbieders van Value Added Networks (VAN's)? Bongers en Steeman geven een verhandeling over de kansen en de bedreigingen van EDI met betrekking tot de strategische positie van het bankwezen.**

## INLEIDING

Electronic Data Interchange is een vorm van telematica waarvan de toepassing steeds verder in het bedrijfsleven raakt ingeburgerd. Zij heeft betrekking op de informatiestroom inzake de logistieke en financiële afhandeling van transacties.

Het bankwezen is als intermediair in het betalingsverkeer dikwijls betrokken bij de financiële afhandeling van transacties tussen partijen. Dat de banken ook een belangrijke rol zouden kunnen spelen in de verdere ontwikkeling van EDI-toepassingen op dit terrein ligt dan ook voor de hand.

Gezien de initiatieven die zijn genomen op het gebied van normalisatie van financiële berichten conform EDIFACT, nemen de banken deze rol serieus [Sonn91]. De oprichting van EDIFIST in mei 1991 waarmee de banken gezamenlijke voorbereiding en ondersteuning van de implementatie van financiële berichten nastreven, bevestigt dit.

Over de concrete invulling van haar rol bestaat echter nog onduidelijkheid. Samenwerking op technisch gebied ontbreekt bijvoorbeeld. Een reden hiervoor zou kunnen zijn dat de strategische aspecten van financiële EDI nog niet zijn uitgekristalliseerd en de gevolgen van EDI voor de individuele banken nog moeilijk zijn te overzien.

Dit artikel tracht een antwoord te vinden op de vraag of EDI strategische waarde heeft voor de banken en hoe banken EDI kunnen gebruiken voor het realiseren van hun eigen bedrijfsdoelstellingen.

## EEN BEGRIPPENKADER

In deze paragraaf worden enkele begrippen rond EDI uitgewerkt. Daarbij is met name van belang dat EDI impliceert dat organisaties besloten hebben samen te werken. Aan de orde komen zowel het netwerk dat voor EDI wordt opgezet in technische zin, als de consequenties van EDI in strategisch opzicht.

### Het computernetwerk

In technische zin wordt met EDI communicatie verwezenlijkt tussen applicaties waarbij berichten worden uitgewisseld en geïnterpreteerd zonder tussenkomst van personen. Een telecommunicatienetwerk waarop onafhankelijke computersystemen zijn aangesloten, zorgt voor de gegevensoverdracht. De software die zorgt voor acceptatie en verzending van berichten en voor de inhoudelijke vertaalslag naar de eigen applicaties, wordt het EDI-systeem genoemd.

De technische componenten - de applicaties, de EDI-systemen en het telecommunicatienetwerk - vormen te zamen een computernetwerk.

Voor dit netwerk moeten in de eerste plaats afspraken worden gemaakt over de gegevensoverdracht. De benodigde compatibiliteit kan een probleem zijn. Het OSI-referentiemodel presenteert deze problematiek in zeven lagen. De huidige netwerkarchitecturen zijn in staat bestaande incompatibiliteit laag voor laag op te lossen. De overdracht van berichten van afzender naar eindbestemming wordt steeds transparanter dankzij interventie van het netwerk. VAN's verzorgen een complete koppeling.

*Administratieve integratie betekent dat tussen processen een brug wordt geslagen, waardoor de problematiek om de gegevensstroom van het ene proces te transformeren naar de gegevensstroom van het andere proces, wordt geminimaliseerd.*

Het compatibiliteitsprobleem blijft echter relevant voor de interconnectivity van de verschillende netwerken. Om tot open communicatie te komen zijn standaardprocedures ontwikkeld. Deze zogenaamde protocollen beschrijven de overdracht per OSI-laag. X.400 beschrijft de koppeling van de bovenste vier lagen. Dit protocol is ontwikkeld voor electronic mail en bevat regels voor bijvoorbeeld de envelop en adressering. Een speciaal voor EDI ontwikkeld protocol is P-edi, dat ook regels bevat voor de structuur van de inhoud van de envelop, waardoor het kunnen doorzenden van berichten en de beveiliging beter gestalte hebben gekregen.

Kenmerkend voor EDI is dat er ook afspraken moeten worden gemaakt over de betekenis van de te verzenden berichten. Om de vertaalslag die elk EDI-systeem moet maken zo eenvoudig mogelijk te houden, is standaardisatie in dit opzicht van groot belang.

In 1987 is de EDIFACT-syntaxis (EDI-standards For Administration, Commerce and Trade) geaccepteerd als internationale norm. De syntax is uitgebreid met een verzameling gegevens- en berichtenomschrijvingen.
Kenmerkend voor deze "EDI-taal" is de onafhankelijkheid ten opzichte van de afspraken over de wijze waarop de gegevensoverdracht plaatsvindt.

Per bedrijfstak zijn EDI-organisaties opgericht die de berichten die voor de eigen doelgroep van belang zijn, uitwerken in subsets. Zij geven advies aan de aangesloten bedrijven inzake de keuze van een netwerk of van software. Sommige EDI-organisaties ontwikkelen ook zelf software en/of beheren een eigen netwerk. Voorbeelden zijn UAC-Transcom in de detailhandel en distributie, en EDIFIST in de banksector.
De mate waarin de algemene normen worden gehanteerd, bepaalt de openheid of geslotenheid van het EDI-systeem. Naarmate een EDI-systeem zich sluit is het geschikter voor heel specifieke toepassingen en/of voor een beperkte groep deelnemers.

### Externe integratie

De uitgebreide definitie van EDI zou kunnen luiden:
*"De elektronische uitwisseling van gestructureerde en genormeerde gegevens tussen computersystemen van organisaties, ten behoeve van het afhandelen van transacties, waarbij externe integratie van het administratieve proces tot stand komt".*

Dit is meer dan een elektronische exercitie "waarbij geen mens meer nodig is". Het venijn zit hem in de staart.
Administratieve integratie betekent dat tussen processen een brug wordt geslagen, waardoor de problematiek om de gegevensstroom van het ene proces te transformeren naar de gegevensstroom van het andere proces, wordt geminimaliseerd. Door stroomlijning van informatie-overdracht worden de processen één geheel. Alleen dan is werkelijk sprake van EDI.

Elk EDI-systeem waarmee de betrokken applicaties met het netwerk zijn verbonden, maakt de vertaalslag van het standaardbericht naar input voor de eigen applicaties en terug. Dankzij deze brugfunctie wordt het administratieve proces één geheel.
Tegelijkertijd behouden de applicaties hun autonomie. Tijdens de communicatie (in het telecommunicatienetwerk en/of in het EDI-systeem) vindt ontkoppeling in de tijd plaats via het store-and-forward-principe. Berichten worden opgeslagen in een postbus. De applicaties hoeven niet op elkaar

te wachten maar kunnen elk, op het moment dat het hen uitkomt, berichten verzenden en ophalen.

Deze ogenschijnlijke paradox van externe integratie met behoud van autonomie heeft de weg vrijgemaakt voor de ontwikkeling van EDI. Brevoord [Brev81] noemde in 1981 het oplossen van alle vertaalproblemen tussen administratieve processen "zeker niet illusoir in situaties waarin computers onderling informatie aan elkaar doorgeven". EDI is nu de elektronische techniek die deze gedachte in praktijk brengt.

Overigens brengt dit met zich mee dat alleen gegevensuitwisseling waarbij de berichten zelfstandige betekenis hebben, geschikt is voor EDI. Gegevensuitwisseling in de vorm van een dialoog via een postbus is op zijn minst omslachtig te noemen.

**Voordelen van EDI**

In eerste instantie speelt vooral de - technische - realisatie van communicatie zonder menselijke tussenkomst een grote rol: EDI betekent vervanging van papieren berichten door elektronische berichten. Het vooruitzicht is kostenreductie en efficiëntie. De kostenreductie vloeit ten eerste voort uit de eenmalige invoer van gegevens. Dit leidt tot aanzienlijke besparingen. Een tweede besparing is gelegen in de mogelijkheid om de informatiestroom betreffende de geld- of goederenstroom te versnellen. Geld en goederen krijgen daardoor een hogere omloopsnelheid.

De voordelen van snellere, accurate berichtgeving nemen toe naarmate meer processen van de organisatie in de externe integratie worden betrokken. Men zal daarom streven naar verdere zogenaamde systems integration.
Tegelijkertijd leidt de externe integratie meestal tot een hogere kwaliteit van het gehele proces. Hiermee doen de deelnemers gezamenlijk een strategisch voordeel.

Op de lange duur zullen als gevolg van de toenemende verwevenheid van activiteiten, processen kunnen worden vereenvoudigd: proces simplification.
De mogelijkheden om processen anders te organiseren vloeien met name voort uit de ontkoppeling van de informatiestromen van de goederenstroom. Door berichten vooruit te zenden kunnen zij extra functies vervullen in de administratieve organisatie en de planning van de goederen- en de geldstromen.
De initiatie en verwerking van informatie kan dichter bij de ontstaansbron worden gelegd. Daarmee worden administratieve procedures verkort. Controle op de goederen- en de geldstroom wordt effectiever op het moment dat zij minder hoeft te worden versnipperd en het administratieve proces als een geheel kan worden overzien. Daarbij speelt het vertrouwen in de integriteit (en rechtsgevoeligheid!) van de berichten ook een grote rol.

De verwezenlijking van externe integratie heeft EDI gemaakt tot een "enabling tool" voor vernieuwde samenwerking tussen organisaties. Want een integrale toepassing door de eigen organisatie en door de hele bedrijfsketen kan gevolgen hebben voor de traditionele produkten en processen.
Op dat moment wordt de onderneming voor strategische keuzen geplaatst. Zowel ten aanzien van de inrichting van haar eigen activiteiten als van haar plaats (haar totale activiteit) ten opzichte van die van anderen. De relatieve open- of gesloten-heid van het EDI-systeem en van het communicatienetwerk is in dit licht een belangrijke keuze.

*Een integrale toepassing van EDI door de eigen organisatie en door de hele bedrijfsketen kan gevolgen hebben voor de traditionele produkten en processen.*

**Het organisatienetwerk**

De intentie om, met behulp van EDI, processen met elkaar te integreren leidt tot de vorming van netwerken van organisaties. Deze kunnen worden beschouwd als een mesoniveau tussen de markt (macro) en de individuele organisatie (micro). Elk organisatienetwerk heeft een eigen bestaansreden en bevindt zich binnen bepaalde krachtvelden.

In het organisatienetwerk komt het doel van de samenwerking tot uitdrukking. De deelnemende partijen zullen afspraken maken over welke informatie zal worden uitgewisseld, en over wie aan het netwerk zullen (mogen) deelnemen. Deze afspraken vormen een leidraad voor de technische keuzen die zullen worden gemaakt bij de invulling van het computernetwerk. Of voor de keuze van de te gebruiken berichten-subset en de daarbij te hanteren normen.

De samenwerkingsverbanden zijn altijd gebaseerd op wederzijdse afhankelijkheid (interdependentie).

Producenten en verkopers voegen als "de schakels van een keten" stuk voor stuk waarde toe aan het economisch proces. De schakels voor een bepaalde produktgroep kennen onderling verticale interdependentie; de schakels die vergelijkbare waarde aan een produkt toevoegen (concurrenten) kennen onderling horizontale interdependentie. De netwerken die producenten en/of verkopers onderling vormen kunnen dan ook worden getypeerd als horizontale of verticale netwerken.
Wanneer een horizontaal en een verticaal netwerk één worden is sprake van symbiose. In een symbiotisch netwerk zijn zowel concurrenten als hun gezamenlijke afnemers of leveranciers betrokken.

De interdependentie is het bestaansrecht van elk organisatienetwerk. Op het moment dat het deelnemen aan een organisatienetwerk zowel gemeenschappelijke voordelen biedt als voor elke partij af-

zonderlijke individuele doeleinden en consequenties in zich heeft, ontstaat echter een politieke dimensie. Elke partij moet het deelnemen kunnen inpassen in de eigen strategie en doelstellingen. Een wederkerigheid inzake voordelen (win-win-situatie) is daarom noodzakelijk voor een vruchtbare samenwerking. Er bevindt zich een spanningsveld tussen enerzijds de afhankelijkheid tussen de partijen en anderzijds de individuele doelstellingen of strategieën.

*Er bevindt zich een spanningsveld tussen enerzijds de afhankelijkheid tussen de partijen en anderzijds de individuele doelstellingen of strategieën.*

Het spanningsveld wordt gevoed door de externe integratie van het administratieve proces die met EDI tot stand komt. Daarmee worden kansen gecreëerd voor de wijze waarop een onderneming haar activiteiten kan organiseren. Maar de kansen kunnen tegelijk een bedreiging zijn voor een andere partij. De afspraken voor het computernetwerk betekenen formalisatie van de communicatie. Dit kan bedrijven in hun functioneren ook beperken.

In de eerste plaats ontstaat het gevaar dat, doordat de werking van processen doorzichtiger wordt, functies gaan verschuiven. Afhankelijk van het overwicht dat een partij heeft kan bijvoorbeeld de (lucratieve of kostbare) voorraadvorming van geld en goederen worden verschoven van de ene naar de andere partij in de bedrijfsketen. Ook functies in een administratieve omgeving kunnen verschuiven. De VAN-leverancier bijvoorbeeld zou in de gelegenheid kunnen zijn de berichten die hij overdraagt ook inhoudelijk te bewerken en daarmee een extra dienst aan te bieden. De netwerkleveranciers zijn in dit opzicht zeer zeker ook te beschouwen als een partij in het organisatienetwerk met eigen belangen en invloeden.

In de tweede plaats wordt door geformaliseerde afspraken de handelingsvrijheid van de deelnemers beperkt. Dit heeft met name bij horizontale interdependentie gevolgen. Concurrenten leveren mogelijkheden in om zich van elkaar te onderscheiden. De realisatie van het horizontale netwerk wordt daarom precompetitief genoemd.
Bij een symbiotisch netwerk doet zich de bijzondere omstandigheid voor dat het precompetitief gebied wordt uitgebreid naar de verticale relatie met de klant. Als bijvoorbeeld het ideale ene transparante netwerk zou ontstaan, zullen de netwerkleveranciers zich met aanvullende diensten op de gegevensoverdracht van elkaar moeten onderscheiden.

In het algemeen geldt dat de terughoudendheid die de formalisatie teweeg brengt groter is naarmate de via het netwerk uit te wisselen informatie een wezenlijk onderdeel uitmaakt van de primaire processen van de onderneming [Vlis88].

## FINANCIELE EDI

De banken zijn meestal alleen betrokken bij de financiële afwikkeling van een transactie. De toepassing van EDI op dit traject wordt financiële EDI genoemd. Met betrekking tot de opzet van financiële EDI zijn twee visies relevant: de visie van het bedrijfsleven en de visie van de banken.

### Het gezichtspunt van het bedrijfsleven

Het berichtenverkeer tussen banken en ondernemingen ten behoeve van het financieel afhandelen van transacties leent zich uitstekend voor store-and-forward. Nu EDI-projecten met betrekking tot de logistieke afhandeling van transacties steeds meer gestalte krijgen, wordt door het bedrijfsleven meer aangedrongen op de mogelijkheid de financiële afwikkeling daaraan te koppelen. Wanneer ook de betalingsopdracht en informatie over de betaling met EDI kunnen worden geïntegreerd, is de kring van administratieve afhandeling rond. Dit wordt ook wel aangeduid met de roep "to close the loop".

Transactie-informatie is in de eerste plaats bestemd voor de financiële administratie; de plaats waar de financiële afwikkeling van transacties plaatsvindt. Vervolgens kan de informatie (bottom-up) als input dienen voor andere afdelingen, zoals inkoop, verkoop, en ook de treasury.

Voor de financiële afhandeling van transacties gaat het om de integratie van bankprocessen met in- en verkoopprocessen die zich bij de cliënt afspelen. Een belangrijk aspect is bovendien dat de banken hun intermediaire rol gezamenlijk vervullen. Cliënten van diverse banken zullen via hun eigen bank transacties met elkaar willen afwikkelen. De banken vervullen een intermediaire functie.

Een symbiotisch netwerk zou volledige externe integratie verwezenlijken. Het traject van de communicatie tussen de bank en haar cliënt is daarin opgenomen en zou daarmee een precompetitief karakter krijgen.

### Het gezichtspunt van de banken

Banken hebben zich hoofdzakelijk en reeds in een vroeg stadium bepaald tot horizontale netwerken, met een gesloten karakter en eigen standaarden. SWIFT op internationaal en de BankGiroCentrale op nationaal terrein zijn de meest in het oog springende voorbeelden.

De terughoudendheid die de formalisatie waarmee netwerkvorming gepaard gaat, teweeg brengt is duidelijk voelbaar. Het betalingsverkeer is immers een zeer belangrijk aspect van het bankbedrijf en

de relatie met de cliënt wordt gekenschetst als concurrentiegevoelig.
Bovendien geeft het karakter van de geldstroom voor de banken, als partij in het netwerk, geen aanleiding tot versnelling. De rente-inkomsten worden niet graag opgegeven en in de vertrouwensrol van de banken is behoudendheid op zijn plaats. Door het bedrijfsleven is de banken dan ook een behoudend en volgzaam karakter verweten.

Aan de andere kant zijn door de banken al in een vroeg stadium EDI-achtige produkten ontwikkeld voor de communicatie tussen bank en cliënt: Electronic Banking (EB). Uitgaande van de horizontale gezamenlijke netwerken, hebben de banken onafhankelijk van elkaar getracht via EB-produkten het traject bank-cliënt daaraan te koppelen. Aangezien elke bank haar eigen EB-produkten ontwikkelt op basis van eigen commerciële doelstellingen, is standaardisatie van EB-produkten niet aan de orde geweest.

Bij de eerste generatie EB-produkten lag de nadruk op het ondersteunen van de treasury van de cliënt. Daarbij ging het vooral om informatie van bank richting cliënt.
Bij de systemen die eind jaren tachtig op de markt werden gebracht, is de aandacht verschoven van treasury-ondersteuning naar de integratie van EB met de financiële administratie van de cliënt, door middel van zogenaamde interfaces. Daarmee wordt de doelgroep van EB-produkten sterk uitgebreid, richting financiële administratie en richting het midden- en kleinbedrijf.

De banken zullen naar verwachting trachten hun EB-systemen uit te breiden met een "EDI-interface". Closing the loop zal in de eerste plaats worden gerealiseerd op het traject tussen de financiële afdeling (of treasury) en de bank: het EB-traject. Vervolgens, nadat de bedrijven (met gebruikmaking van het EDIFACT-factuurbericht) hun financiële administratie hebben geïntegreerd met de logistieke transactieverwerking, zal de kring zijn gesloten. De synthese van financiële EDI met logistieke EDI vindt als het ware top-down plaats: vanuit de treasury-functie.

Het resultaat zal zijn dat de externe integratie tussen bankprocessen en de financiële administratie per cliënt zal worden georganiseerd. De banken zorgen ervoor dat hun cliëntenrelaties op zichzelf blijven staan en niet opgaan in een gemeenschappelijke interface voor alle banken versus alle cliënten. Het netwerk blijft een (gesloten) horizontaal netwerk en breidt zich niet uit tot een (open) symbiotisch netwerk.

**Een analyse**

De banken achten de EB-produkten van strategisch belang voor het uitbreiden en intensiveren van de relaties met (potentiële) klanten. De huidige technische mogelijkheden worden in concurrentie met elkaar ontwikkeld en benut. Het vasthouden aan eigen standaarden is daarvoor een indicatie. Daarbij moet worden opgemerkt dat binnen drie jaar nadat het eerste EB-produkt op de markt werd geïntroduceerd, praktisch alle banken een dergelijk produkt op de markt hebben gebracht. De functionaliteit en daarmee ook de doelgroep van de produkten wordt door de banken telkens uitgebreid. Steeds meer cliënten maken van EB-produkten gebruik en het gaat om steeds grotere volumes. Op den duur zal EB zijn geëvolueerd van een specialistische dienstverlening van enkele banken aan een kleine groep topcliënten, tot een standaarddienst van vele banken aan een brede groep gebruikers. In die zin zou de strategische waarde die banken toekennen aan het zelfstandig ontwikkelen van EB-produkten wel eens twijfelachtig kunnen zijn.

Transactioneel verkeer, in casu het verkeer tussen bank en financiële administratie, is geschikt voor EDI vanwege de ontkoppeling in de tijd via het store-and-forward-principe, die daarbij mogelijk is. EB heeft vanuit haar treasury-achtergrond van oorsprong een dialoogkarakter. Zal EB dan wel geschikt blijken om werkelijke integratie te verwezenlijken tussen de administratieve processen van de cliënt en de bank, laat staan van processen van cliënten via de bank?

*De voordelen van externe administratieve integratie manifesteren zich pas echt wanneer de afstemming in de eigen administratieve processen doordringt.*

De voordelen van externe administratieve integratie manifesteren zich pas echt wanneer de afstemming in de eigen administratieve processen doordringt. Dan kunnen interne processen worden gestroomlijnd en doen zich strategische kansen voor om processen of diensten te hergroeperen. Uit-gaande van het EB-concept moeten bij de cliënt echter nog diverse vertaalslagen plaatsvinden. Derhalve komen de mogelijkheden van externe administratieve integratie voor de processen die zich bij de cliënt afspelen, bij dit concept onvoldoende tot hun recht.

## STRATEGISCH PERSPECTIEF

De twee gezichtspunten leiden tot aarzeling bij het verder ontwikkelen van financiële EDI. Gegeven de bovenstaande analyse wordt in deze paragraaf behandeld langs welke weg financiële EDI de banken het meest perspectief biedt op de lange termijn.

**Het open alternatief**

Een alternatief voor het EB-concept zou kunnen zijn dat de banken gezamenlijk een interface bieden aan cliënten, bijvoorbeeld via een EDI-netwerk dat cliënten onderling reeds hebben opgebouwd voor de logistieke transactieverwerking. De bankspecifieke EB-standaarden kunnen dan helemaal worden losgelaten; er is sprake van een open financiële omgeving en een symbiotisch netwerk.

De banken ervaren ontwikkelingen in deze richting in eerste instantie mogelijk als een bedreiging. Bestaat immers niet het gevaar dat dan ook de financiële verplichtingen van verschillende, onafhankelijke ondernemingen rechtstreeks kunnen worden vereffend, buiten de banken om?

Voor ondernemingen betekent financiële EDI integratie van hun systemen, via systemen van de bank. De relatie cliënt-bank/bank-cliënt staat in hun ogen voorop; de bank speelt "slechts" een intermediërende rol in het betalingsverkeer. Bij deze gedachte past de opzet van een symbiotisch netwerk wel. Wanneer banken vasthouden aan hun EB-produkten en moeizaam interfaces trachten te ontwikkelen zouden bedrijven op eigen initiatief hun financiële zaken via open netwerken kunnen gaan regelen.

Wat de banken zich bij het kiezen van een strategie in dezen ons inziens eerst zullen moeten afvragen is of zij, uitgaande van het EB-concept, in staat zullen zijn op lange termijn een toegevoegde waarde (competitive edge) met EDI zullen realiseren. Voor een antwoord op deze vraag moet worden onderzocht waar de strategische waarde van EDI voor de banken ligt. Vervolgens kan een indruk worden gegeven van de dienstverlening die banken zouden kunnen bieden en van de rol die de banken zouden kunnen spelen in de samenwerking met bedrijven, op organisatorisch niveau.

*De integratie met externe systemen heeft niet alleen effecten voor de eigen organisatie; de dienstverlening van de banken als geheel krijgt een impuls.*

**Voordelen van EDI voor de bank**

De voordelen van een EDI-toepassing manifesteren zich in drie fasen:
1. document elimination;
2. systems integration;
3. proces simplification.

*Document elimination*
Voor de banken is een groot efficiëntievoordeel te behalen. Het kostenvoordeel vloeit met name voort uit de eenmalige invoer van gegevens. Deze efficiëntievoordelen zijn niet afhankelijk van het feit of de financiële transactieverwerking via een open EDI-netwerk of via het EB-concept wordt aangeboden.

*Systems integration*
Voor de bank kan de kwaliteit (beschikbaarheid, juistheid, tijdigheid) van de interne informatievoorziening worden verhoogd. Daarmee is betere ondersteuning van interne functies en processen mogelijk.
De integratie met externe systemen heeft niet alleen effecten voor de eigen organisatie; de dienstverlening van de banken als geheel krijgt een impuls. Vooral omdat voor de afwikkeling van financiële transacties de cliënten zijn aangewezen op meer dan alleen hun eigen bank.
Op deze wijze zal EDI kunnen bijdragen aan een verbeterde cliëntgerichte organisatie van de bank.

Voor deze fase is men gebaat bij open systemen en algemene standaarden. Dat geldt met name voor de bedrijven, maar ook voor de banken, wanneer zij de integratie van hun interne processen willen verbeteren en vanuit het back-office nieuwe informatiestromen richting cliënt willen genereren.

*Proces simplification*
De integratie van systemen met behulp van EDI creëert ook voor banken mogelijkheden voor structurele veranderingen in de organisatie van processen, bijvoorbeeld centralisatie van gegevens en decentralisatie van bevoegdheden en/of dienstverlening op basis van beschikbare informatie, en voor nieuwe dienstverlening.

De nieuwe dienstverlening kan als tweeledig worden beschouwd.
Ten eerste kunnen diensten worden ontwikkeld vergelijkbaar met de functies van een inhousebank (netting van verplichtingen, reinvoicing en factoring). Maar nu niet alleen gericht op één concern, maar op een willekeurige groep aangesloten ondernemingen. De dienstverlening van de bank breidt zich uit van handel in geld naar handel in informatie over geld. De banken trekken daarmee een administratieve en financieel risicodragende functie naar zich toe. Deze verschuiving van functies van cliënten naar banken wordt reëel, gezien de tendens tot externalisatie van non-produktieve activiteiten die zich in de markt afspeelt.
Ten tweede kan de bank zich actief opstellen als zogenaamde EDI-enabler en daarmee een optimaal gebruik maken van de bij haar aanwezige expertise op het gebied van bijvoorbeeld beveiliging, communicatie, netwerk- en informatietechnologie.

De banken zullen de intermediërende rol in het betalingsverkeer op deze manier kunnen behouden.
Allereerst dankzij de kennis die bij de banken aanwezig is ten aanzien van elektronische gegevensuitwisseling, met name op het gebied van beveiliging, waardoor de rol van EDI-enabler voor de cliënten een reële waarde kan krijgen. Maar vooral

vanwege de vertrouwensrelatie en het financiële draagvlak die voor de risicobemiddeling nodig zijn en die vanouds het hart van het bankwezen vormen.
Anderzijds zullen cliënten zich minder gebonden voelen aan een "eigen" bank en zal de concurrentie tussen de banken zich scherper aftekenen, omdat de informatie over tarieven en de toegankelijkheid van de betaaldiensten voor de cliënten optimaal is geworden.

EB is van oorsprong een dienstverlening aan de grote bedrijven. Netting, inhouse-banking speelt daar een steeds grotere rol. Interfaces ten behoeve van financiële EDI zullen hoogstwaarschijnlijk het eerst voor deze klanten tot stand komen.
De bottom-up benadering betekent dat de banken zich expliciet kunnen richten op het midden- en kleinbedrijf; een relatief onontgonnen terrein met hoge aantallen transacties.

Het belang van de informatie over de betaling zou ook aanleiding kunnen zijn om de financiële EDI per EDI-organisatie te regelen (net zoals de inhouse-bank per EDI-organisatie zou worden opgezet). Per EDI-organisatie bestaat een verschillende behoefte aan specifieke toevoegingen. Iedere bank kan de band met haar eigen specifieke doelgroepen op die manier trachten te versterken.

Bovenop de intermediaire rol kan de bank de cliënten aan zich binden door serviceverlening op EDI-gebied en informatiediensten ten behoeve van de financiële afwikkeling van transacties.

## CONCLUSIES

Uit het voorgaande kan worden geconcludeerd dat de banken de competitive edge niet moeten zoeken in de infrastructuur ten opzichte van de EDI-diensten voor het betalingsverkeer. Zij zullen haar moeten zoeken in produktinnovaties die mogelijk worden dankzij de infrastructuur.

Electronic Banking (EB)-produkten zullen niet de diensten blijven waarmee men zich in technische zin differentieert. Men zal voor het betalings- en documentenverkeer gebruik moeten maken van open datacommunicatiestructuren.
EB zal als een "poort" moeten gaan functioneren van een symbiotisch netwerk van banken en bedrijven. Dit netwerk zal de banken de mogelijkheid geven hun dienstenniveau te optimaliseren, hun eigen kosten te verlagen en een competitive edge te ontwikkelen in service, financiële deskundigheid en dienstverlening op het terrein van de risicobemiddeling. De produktinnovaties zullen kunnen leiden tot nieuwe dienstverlening waarmee zij de oorspronkelijke kernactiviteit (financing, risicobemiddeling) kunnen uitbreiden.

Zolang de banken deze conclusie niet trekken, zal het EB-produkt uiteindelijk niet meer zijn dan een communicatiemedium dat de post heeft vervangen. Een produkt dat een zekere kwaliteitsverbetering heeft bewerkstelligd in de wijze waarop cliënten informatie met de banken kunnen uitwisselen, maar waarmee de banken geen wezenlijke verbetering van hun concurrentiekracht hebben kunnen initiëren.

De vereiste win-win-situatie speelt met name een rol tussen de banken onderling. De banken zullen ieder voor zich in het gegeven dat het dienstenniveau van het bankwezen als geheel een impuls krijgt, een individueel voordeel moeten zien in de vorm van het realiseren van een nieuwe dimensie in de strategic edge van de eigen onderneming.
Met name grotere banken zullen zich dienen te realiseren dat zij door het publiek worden beoordeeld op de kwaliteit en prijs van hun financing-activiteiten, en dat cliënten hun keuzevrijheid, hun onafhankelijkheid, daarin niet zullen willen verliezen. Banking zal zich verder ontwikkelen als de elektronische interface tussen banken - als groep - en hun gezamenlijke cliënten.

## LITERATUUR


[Bala90] Drs. Ph.J.R. Balakirsky, *Een uitdaging voor banken: Electronic Data Interchange,* Bank- en Effectenbedrijf, december 1990.

[Brev81] Prof.dr. C. Brevoord RA en drs. H. Gorter de Vries, *Externe Administratieve Integratie,* Stenfert Kroese, 1981.

[Door91] R. van Doorn, *Het moeizame (financiële) traject van EDI; "De vraag vanuit de markt is niet duidelijk",* Telecommagazine, 1991/6.

[Hamm90] M. Hammer, *Reengineering Work: Don't Automate, Obliterate,* Harvard Business Review, July-August 1990.

[Scha90] R.P.G. van Schaik, H.H.G. Smorenberg en drs. D.M. Swagerman, *Elektronisch bankieren, de praktijk voor bank en bedrijf,* Delwel Uitgeverij B.V., 1990.

[Sonn91] Dr. M.A.A. Sonnemans en A.T.C. Siebbeles, *Telebankieren met EDI,* Informatie, 1991/11.

[Vlis88] Ir. P. van der Vlist, *Telematica Netwerken; een organisatorisch perspectief,* Tutein Nolthenius, 1988.

[Zand89] Drs. Chr.J. Zanders, *Elektronisch bankieren: een uitdaging,* Financieel Management, 1989/6.



*Drs. M.A. Bongers RE*
*Is hoofd EDP-Audit bij de Interne Accountants Dienst van Credit Lyonnais Bank Nederland N.V.*
*Daarnaast is hij bestuurslid van de Nederlandse Orde van Register EDP-Auditors (NOREA). Tevens is hij lid van de programmacommissie van de EDP-Audit-opleiding aan de Vrije Universiteit te Amsterdam.*

*Mw. drs. M. Steeman*
*Studeerde maart 1992 af aan de economische faculteit van de Vrije Universiteit te Amsterdam in de Bestuurlijke Informatiekunde; onderwerp scriptie: financiële EDI. Sinds 1 april 1992 is zij werkzaam bij Wavin te Hardenberg, afdeling Informatievoorziening.*

# Beheersing van inzet en gebruik IT: van kopzorg tot hoofdzaak

## Een aanpak voor het management

Drs. G.C.M. Mol en drs. J.F.H. Vrins

**Hoewel de gevolgen van ondoordacht gebruik van IT meer dan bekend zijn blijken lijnmanagers nog altijd onvoldoende te zijn betrokken bij IT-gebruik.**
**Ontbreekt het hen aan een aanpak? Mol en Vrins zetten op pakkende wijze uiteen hoe het lijnmanagement zijn greep op de steeds verder geautomatiseerde informatievoorziening kan (her)winnen.**

## INLEIDING

Het management van veel organisaties is nog onvoldoende betrokken bij de kwaliteitsbeheersing van de (veelal geautomatiseerde) informatievoorziening. Vreemd eigenlijk, want juist een goede informatievoorziening en de daarbinnen toegepaste informatietechnologie (IT) spelen een steeds belangrijkere rol bij de realisatie van de bedrijfsdoelstellingen. Corporate networks, vluchtreserveringssystemen, EDI, enz. hebben het (strategische) belang van IT voor organisaties al lang bewezen.

Met name de toepassing van IT in belangrijke primaire processen, zoals inkoop, produktie en verkoop, heeft sterk bijgedragen aan een vergroting van de afhankelijkheid van organisaties van IT. Desondanks vinden de inzet en het gebruik van IT binnen organisaties nog te veel onbeheerst plaats. In dit artikel wordt een aanpak gepresenteerd waarmee het management de toepassing van IT binnen organisaties beter kan beheersen.

## MANAGEMENT EN IT

De ontwikkelingen van de laatste jaren op het gebied van IT hebben ervoor gezorgd dat de toepassing ervan binnen organisaties ieder jaar groter is geworden. Was de toepassing van IT in het verleden alleen nog maar gericht op de administratieve processen, tegenwoordig speelt IT binnen vrijwel alle bedrijfsprocessen een belangrijke rol. Zoals hierboven reeds is gezegd, heeft met name de toepassing van IT bij belangrijke primaire bedrijfsprocessen sterk bijgedragen aan een vergroting van de afhankelijkheid van organisaties van de (geautomatiseerde) informatievoorziening.
Deze afhankelijkheid kan verstrekkende gevolgen hebben voor een organisatie. Het management[1] van organisaties dient zich goed te realiseren wat de gevolgen zijn voor:

- een financiële instelling als het corporate network "down" gaat;
- een luchtvaartmaatschappij als het vluchtreserveringssysteem niet meer betrouwbaar functioneert;
- een transportonderneming als het nieuw ontwikkelde EDI-systeem niet voldoet aan de eisen van de belangrijkste klanten;
- een grootwinkelbedrijf als de gegevens in de centrale database van het kassa-scanning-systeem plotseling verdwenen blijken te zijn.

Bovenstaande voorbeelden bevestigen het geschetste beeld dat organisaties steeds afhankelijker worden van IT.

Deze toenemende afhankelijkheid heeft geleid tot een sterke bewustwording bij het management en extra aandacht voor de inzet en het gebruik van IT. Op dit moment is dan ook een verschuiving waar te nemen van taken en verantwoordelijkheden met betrekking tot IT van de stafafdelingen naar de lijnorganisatie. Echter, uit gesignaleerde problemen in de praktijk blijkt dat ondanks deze extra aandacht het gebruik en de inzet van IT binnen organisaties nog onbeheerst plaatsvinden. Enkele voorbeelden hiervan zijn:

- laag rendement op IT-investeringen;
- realisatie van informatieplannen loopt niet goed;
- verstoorde relatie tussen de automatiseringsafdeling en de rest van de organisatie;
- ontwikkeling van (geautomatiseerde) informatiesystemen loopt qua kosten, tijd en kwaliteit (nog steeds) uit de hand;
- ontevredenheid bij eindgebruikers;
- meer onderhoud aan dan ontwikkeling van informatiesystemen.

## DOEL ARTIKEL

Uit het voorgaande moge duidelijk zijn dat het management van veel organisaties de grip op de (geautomatiseerde) informatievoorziening heeft verloren, mocht het deze ooit hebben gehad. Dit wordt met name veroorzaakt door het ontbreken van een goede aanpak, waarmee het management de taken en verantwoordelijkheden ten aanzien van de beheersing van deze informatievoorziening kan dragen.

In dit artikel wordt een aanpak besproken, waarmee het management zicht krijgt op de kwaliteit van de belangrijkste delen van de (geautomatiseerde) informatievoorziening binnen de organisatie. De aanpak is opgesteld op basis van praktijkervaringen en resulteert in periodieke managementinformatie over de gewenste kwaliteit van de informatievoorziening versus de werkelijke kwaliteit. Op basis van deze informatie kan het management (indien nodig) corrigerende acties nemen ter verbetering van de beheersing.

### Informatietechnologie

In de literatuur is (nog) geen eenduidige definitie van informatietechnologie (IT) voorhanden. In dit artikel wordt uitgegaan van een algemene definitie, zoals die door Hopstaken en Kranendonk wordt gehanteerd:

*"Informatietechnologie is de technologie van het vastleggen, bewerken en opslaan van gegevens en het verschaffen van informatie"* [Hops92].

Omdat de toepassing van IT binnen organisaties heeft geleid tot een verregaande automatisering van de informatievoorziening worden de begrippen IT en (geautomatiseerde) informatievoorziening in dit artikel als synoniemen gebruikt.

### Opbouw artikel

In dit artikel wordt allereerst ingegaan op het beheersingsvraagstuk van de (geautomatiseerde) informatievoorziening. Vervolgens wordt een management-aanpak gepresenteerd waarmee het management voldoende grip kan krijgen op de kwaliteitsbeheersing van de (geautomatiseerde) informatievoorziening. De aanpak wordt aan de hand van een voorbeeld toegelicht. Verder wordt kort ingegaan op de ondersteuning van het management bij deze beheersing door deskundigen. Tot slot worden de belangrijkste conclusies nog eens op een rijtje gezet.

## BEHEERSINGSVRAAGSTUK IT

Voor een goede uitvoering en beheersing van de bedrijfsprocessen heeft men binnen iedere organisatie informatie nodig. Deze informatie dient te voldoen aan de eisen van de bedrijfsprocessen die gebruik maken van die informatie. Deze eisen worden ook wel aangeduid als kwaliteitseisen[2].
Voorbeelden van kwaliteitseisen zijn eisen aan de mate van betrouwbaarheid of snelheid van de opgeleverde informatie.
Om beter te kunnen voldoen aan de eisen van de bedrijfsprocessen wordt door organisaties op steeds grotere schaal gebruik gemaakt van IT binnen de informatievoorziening (automatisering van

1. *Waar in dit artikel wordt gesproken over management wordt steeds bedoeld het lijnmanagement van een organisatie op de verschillende hiërarchische niveaus (strategisch, tactisch en operationeel).*
2. *In dit artikel wordt onder kwaliteitseisen verstaan: de verzameling van eisen aan de informatievoorziening, dat wil zeggen zowel functionaliteitseisen als gedrags- en prestatie-eisen.*

de informatievoorziening). Of een organisatie erin slaagt de informatie te laten voldoen aan de genoemde kwaliteitseisen is afhankelijk van de wijze waarop zij geautomatiseerde informatievoorziening beheerst. Met andere woorden, voor een optimale uitvoering en beheersing van de bedrijfsprocessen dient de geautomatiseerde informatievoorziening van deze processen in voldoende mate te worden beheerst.

*Beheersen van de (geautomatiseerde) informatievoorziening wordt in dit artikel gedefinieerd als het zodanig plannen, uitvoeren, beheren en bijsturen van de (geautomatiseerde) informatievoorziening dat de kwaliteit van de informatie (blijvend) voldoet aan de eisen van de organisatie.*

Daarbij dient nader te worden omschreven wat onder het begrip kwaliteit wordt verstaan.

*Kwaliteit wordt in dit kader gedefinieerd als de mate waarin het geheel van eigenschappen van een produkt, proces of dienst voldoet aan de eraan te stellen eisen, welke voortvloeien uit het gebruiksdoel* [NNI80].

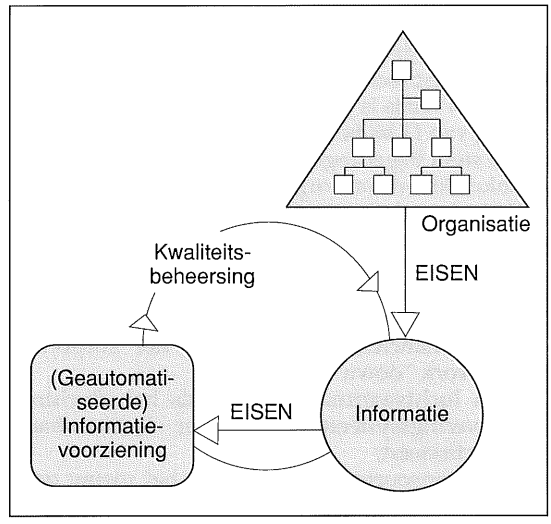
Kwaliteit wordt vertaald als het produkt van effectiviteit (de mate van doelrealisatie) en efficiëntie (de mate van doelmatigheid) [Moon91]. Omdat de begrippen effectiviteit en efficiëntie van een vrij hoog abstractieniveau zijn, dienen deze begrippen voor een praktische invulling van het beheersingsvraagstuk te worden vertaald in meer concrete kwaliteitsattributen. Een bekend voorbeeld van een indeling in kwaliteitsattributen wordt gegeven door Delen en Rijsenbrij [Dele90].

Een vaste indeling in kwaliteitsattributen is in deze algemene benadering van kwaliteitsbeheersing echter niet zinvol. Afhankelijk van de specifieke eisen van een organisatie zullen de begrippen effectiviteit en efficiëntie moeten worden vertaald naar kwaliteitsattributen die voor die organisatie de beste invulling vormen van deze begrippen.

**Opbouw beheersingsvraagstuk**

Om inzicht te krijgen in de beheersing van de (geautomatiseerde) informatievoorziening is de opbouw van het beheersingsvraagstuk van belang. Hierbij wordt allereerst een onderscheid gemaakt tussen de informatievoorziening als proces en het produkt van de informatievoorziening, te weten informatie. De beheersing van de kwaliteit van de informatie (het produkt) is sterk afhankelijk van de beheersing van de informatievoorziening (het proces). Indien een organisatie bijvoorbeeld de betrouwbaarheid van het informatievoorzieningsproces onvoldoende beheerst, zijn er vanzelfsprekend weinig waarborgen voor de betrouwbaarheid van de opgeleverde informatie.
Het volgende voorbeeld zal het een en ander verduidelijken. Indien de auto's die door een autofabrikant worden geproduceerd aan hoge veiligheidseisen dienen te voldoen (bijvoorbeeld bepaald door wetgeving of markteisen), dan dient het fabricageproces zodanig te worden beheerst dat dergelijke auto's ook daadwerkelijk worden gefabriceerd.

De kwaliteitseisen die aan de produkten (auto's of informatie) worden gesteld, dienen te worden vertaald naar kwaliteitseisen aan het proces (fabricageproces of informatievoorzieningsproces). Door een beheersing van het proces heeft een organisatie grip op de kwaliteit van het produkt (zie figuur 1).




*Figuur 1. Het beheersingsvraagstuk.*

Indien het informatievoorzieningsproces vervolgens gedetailleerder in kaart wordt gebracht, dan blijkt dit proces opgebouwd uit een cyclus van deelprocessen en (tussen)produkten (zie figuur 2). Deze deelprocessen spelen zich gedeeltelijk af in de gebruikersorganisatie en gedeeltelijk in de automatiseringsorganisatie. Voor een goede beheersing van de informatievoorziening is deze cyclus belangrijk. Door de toegenomen complexiteit van de geautomatiseerde informatievoorziening en de afhankelijkheid van organisaties van deze informatievoorziening, dienen organisaties voldoende aandacht te besteden aan de kwaliteitsbeheersing van alle deelprocessen en tussenprodukten.

Te vaak nog besteden organisaties vrijwel alleen aandacht aan de deelprocessen analyseren/ontwerpen, bouwen en exploiteren/beheren. Juist het periodiek evalueren en het zorgvuldig plannen van de informatievoorziening blijken in de praktijk twee van de succesfactoren te zijn voor een beheerste informatievoorziening en dus voor een goede ondersteuning van de bedrijfsprocessen.

## EEN MANAGEMENT-AANPAK

Zoals bij het beheersingsvraagstuk reeds is beschreven, zijn de inzet en het gebruik van IT gericht op de ondersteuning van de bedrijfsprocessen. Doordat meestal niet alle bedrijfsprocessen voor een organisatie van even groot belang zijn, kent iedere organisatie kritieke bedrijfsprocessen. Vanwege het belang van de kritieke bedrijfsprocessen voor de onderneming dient de informatievoorziening deze processen goed te ondersteunen. Be-

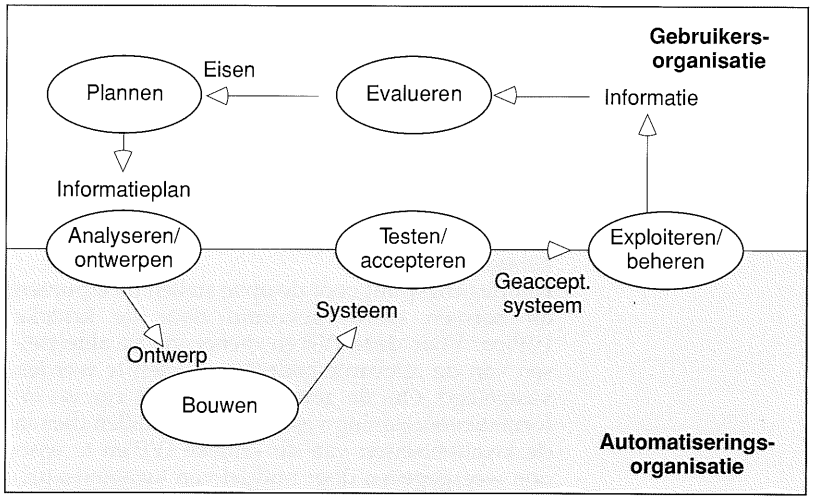
paalde delen van de informatievoorziening zijn daarom belangrijker dan andere voor de ondersteuning van de bedrijfsprocessen en het bereiken van de bedrijfsdoelstellingen. Zo zal een handelsonderneming die sterk afhankelijk is van haar inkoop- en verkoopproces relatief veel aandacht besteden aan de beheersing van de geautomatiseerde informatievoorziening van het inkoop- en verkoopproces. Het management van deze organisatie kiest daarbij impliciet om bepaalde delen van de informatievoorziening niet of minder goed te beheersen, bijvoorbeeld doordat de kosten van beheersing hoger zijn dan het te verkrijgen nut.

**Het opstellen van de management-aanpak**

Voor een goede uitvoering van zijn taken en het kunnen dragen van de daarbij behorende verantwoordelijkheden dient het management te beschikken over een aanpak waarmee het de kwaliteit van de (geautomatiseerde) informatievoorziening binnen zijn organisatie kan beheersen.
De in dit artikel beschreven management-aanpak bestaat uit een vijftal stappen. De aanpak levert een stelsel van meetpunten op in de informatievoorziening waarmee het management een vinger aan de pols kan houden bij de kwaliteit van de belangrijkste informatievoorzieningsprocessen (IVP'en). Aan de hand van periodieke metingen verkrijgt het management informatie over de kwaliteit van de informatievoorziening en kan het desgewenst acties ondernemen ter verbetering van de beheersing.

*Stap 1.*
*Vastleggen doelstellingen informatievoorziening*
Het uitgangspunt voor de management-aanpak wordt gevormd door de doelstellingen van de onderneming en de daaruit afgeleide doelstellingen van de (geautomatiseerde) informatievoorziening. Hierin dient immers te zijn opgenomen welke rol de (geautomatiseerde) informatievoorziening heeft in relatie tot het ondernemingsbeleid en welke delen van de informatievoorziening van (strategisch) belang zijn voor de organisatie. Het management dient de doelstellingen van de (geautomatiseerde) informatievoorziening vast te leggen in het informatiebeleid.

De doelstellingen van de informatievoorziening kunnen verschillend zijn en zijn daarnaast aan verandering onderhevig [Grev89]. Ter verduidelijking volgt hieronder een aantal voorbeelden van (mogelijke) doelstellingen. Organisaties die aan het begin van de toepassing van IT staan, richten zich veelal op het bereiken van kostenbesparingen door de toepassing van IT. In een volgend stadium wordt IT vaak toegepast om knelpunten op te lossen en om de effectiviteit van de bedrijfsprocessen te verbeteren. Veel organisaties zien zich door de complexiteit en de concurrentie van de markt genoodzaakt om meer flexibel en klantgericht te functioneren. Dit veroorzaakt een explosie van (steeds veranderende) informatiebehoeften binnen organisaties. De geautomatiseerde informatievoorziening dient de veranderingen in de bedrijfsprocessen te kunnen volgen zodat zij de bedrijfsprocessen goed kan blijven ondersteunen. Tegenwoordig wordt IT door organisaties vaak toegepast om zich te kunnen onderscheiden van concurrenten. De geautomatiseerde informatievoorziening is dan gericht op het behalen van concurrentievoordelen.




*Figuur 2. Deelprocessen en tussenprodukten van het informatievoorzieningsproces.*

Het resultaat van stap 1 is een expliciete vastlegging van de doelstellingen van de (geautomatiseerde) informatievoorziening.

*Stap 2.*
*Het afbakenen van kritieke IVP'en*
Zoals aan het begin van deze paragraaf reeds is aangegeven, zijn bepaalde IVP'en voor een organisatie van groter belang dan andere en verdienen daarom uit het oogpunt van beheersing extra aandacht.

Voor de afbakening van kritieke IVP'en dienen allereerst alle IVP'en van een onderneming in kaart te worden gebracht. Vervolgens dienen de doelstellingen van de individuele IVP'en te worden beschreven. Aan de hand van de doelstellingen van de informatievoorziening (stap 1) kan nu worden bepaald welke IVP'en kritisch zijn voor een onderneming. Een IVP dient daarbij als kritisch te worden aangemerkt indien het realiseren van de doelstellingen van de informatievoorziening in belang-

*Veel organisaties zien zich door de complexiteit en de concurrentie van de markt genoodzaakt om meer flexibel en klantgericht te functioneren. Dit veroorzaakt een explosie van (steeds veranderende) informatiebehoeften binnen organisaties.*

rijke mate afhankelijk is van de mate waarin de doelstelling van het IVP wordt gerealiseerd.

Het resultaat van stap 2 is een beschrijving van de kritieke IVP'en van een organisatie.

*Stap 3.*
*Het ontwikkelen van een stelsel van meetpunten en normen*
Het uitgangspunt voor de op te stellen meetpunten en normen wordt gevormd door de kritieke IVP'en. Voor deze IVP'en dienen de kwaliteitseisen van de relevante bedrijfsprocessen te worden vastgelegd. Om de gewenste kwaliteit van de informatievoorziening vast te kunnen stellen dienen de kwaliteitseisen van de kritieke IVP'en te worden weergegeven door middel van kwaliteitsattributen. De meetpunten worden opgesteld door deze kwaliteitsattributen zoveel mogelijk te vertalen in meer concrete prestatie-indicatoren. Indien de prestatie-indicatoren op een meetbaar niveau zijn opgesteld, vormen zij de meetpunten voor de management-aanpak. Zo kan bijvoorbeeld het aantal fouten in de facturen als één van de prestatie-indicatoren dienen voor het kwaliteitsattribuut betrouwbaarheid.

*Bij de vaststelling van normen dient het management zich te realiseren dat deze normen aan verschillende bronnen kunnen worden ontleend, zoals wet- en regelgeving, bedrijfskundige principes, en ook de ondernemingsstrategie.*

Per meetpunt (en dus per prestatie-indicator) dient door het management van de organisatie een norm te worden bepaald. Bij het zojuist gegeven voorbeeld kan als norm het aantal foutieve facturen per tijdseenheid worden genomen (bijvoorbeeld maximaal tien per week) of het percentage onjuiste facturen van het totale aantal verwerkte facturen (bijvoorbeeld maximaal vier procent). Bij de vaststelling van normen dient het management zich te realiseren dat deze normen aan verschillende bronnen kunnen worden ontleend, zoals wet- en regelgeving, bedrijfskundige principes, en ook de ondernemingsstrategie. Kwaliteitsnormen kunnen zowel objectief als subjectief bepaald zijn [NGI88]. Daarnaast ligt aan de definitie van een goed normenstelsel een leerproces ten grondslag. In de loop van de tijd zullen de kwaliteitsnormen steeds nauwkeuriger kunnen worden vastgesteld en bieden ze een steeds betere toetsingsbasis voor het management.
Stap 3 resulteert in een vastlegging van het stelsel meetpunten en bijbehorende normen voor de kritieke IVP'en.

*Stap 4.*
*Het uitvoeren van periodieke metingen*
Aan de hand van het in stap 3 opgestelde stelsel meetpunten dienen periodiek metingen ten aanzien van de kwaliteit van de kritieke IVP'en te worden uitgevoerd. Daarbij worden de resultaten van de metingen (de werkelijke kwaliteit) per prestatie-indicator vergeleken met de gedefinieerde normen (gewenste kwaliteit). Uit de metingen blijkt voor welke IVP'en de kwaliteit in voldoende mate wordt beheerst en voor welke IVP'en de kwaliteit tekort schiet. Deze laatste gebieden vormen signalen voor het management om de beheersingsaanpak aan te passen (zie stap 5).

Het resultaat van stap 4 is (periodieke) management-informatie over de kwaliteit van de kritieke IVP'en.

*Stap 5.*
*Het doorvoeren van verbeteringen in de beheersingsaanpak*
Voor de beheersing van de geautomatiseerde informatievoorziening zijn diverse beheersingsmiddelen beschikbaar, zoals planning, budgettering en interne controle. Het inzetten van beheersingsmiddelen geeft echter nog geen garantie voor de beheersing van de kwaliteit. De beheersingsmiddelen dienen efficiënt en effectief te worden ingezet. Met behulp van de stappen 1 tot en met 4 verkrijgt het management informatie over de kwaliteit van de kritieke IVP'en. Voor de IVP'en waarbij de werkelijke kwaliteit afwijkt van de norm dient te worden geanalyseerd wat hiervan de oorzaak is.
Aan de hand van deze analyse kan het management de beheersingsaanpak, zijnde de verzameling van toegepaste beheersingsmiddelen, aanpassen zodat een betere beheersing van de IVP'en wordt gewaarborgd.

**Periodieke beoordeling management-aanpak**

Periodiek dient het management te beoordelen of de toegepaste management-aanpak nog actueel is. De uitgangspunten op basis waarvan de aanpak is opgesteld, kunnen namelijk zijn veranderd. Zo kunnen de doelstellingen van de informatievoorziening veranderd zijn en niet geheel meer overeenkomen met de doelstellingen ten tijde van het opstellen van de management-aanpak. Indien dit het geval is, zal het management de stappen 1 tot en met 5 opnieuw dienen te doorlopen om zodoende de management-aanpak aan te passen aan de veranderde omstandigheden.

## EUROTRANS BV

Ter verduidelijking wordt in deze paragraaf de management-aanpak toegelicht aan de hand van een voorbeeld.

### Algemeen

Eurotrans BV is een middelgrote transportonderneming. De markt waarin Eurotrans opereert is te typeren als een sterk dynamische markt met felle concurrentiestrijd en daardoor lage winstmarges. Om succesvol te kunnen zijn in deze markt is het belangrijk snel te reageren op nieuwe transportopdrachten van klanten. Dagelijks voert de verkoopafdeling overleg met de klanten over de uitvoering van nieuwe en lopende transportopdrachten (vertrek- en aankomsttijden, locaties, eventuele vertragingen, etc.). Door de dynamiek van de markt hanteert het verkoop-management van Eurotrans korte-termijnverkoopdoelstellingen, die op basis van management-informatie regelmatig worden bijgestuurd.

Omdat zowel van buiten de onderneming (leveranciers en klanten) als van binnen de organisatie (afdeling Verkoop, Logistiek en Financiële Administratie) allerlei signalen komen dat de informatievoorziening niet voldoet aan de eisen, besluit de directie van Eurotrans eind 1989 iets te doen aan de toenemende klachten met betrekking tot de (geautomatiseerde) informatievoorziening.

Teneinde de informatievoorziening beter te beheersen besluit de directie om de automatiseringsafdeling een informatieplan te laten opstellen, eventueel samen met een aantal gebruikers. In januari 1990 wordt een budget toegewezen en het project "Infoplan '90" gaat van start. Na anderhalf jaar, "Infoplan '90" is inmiddels omgedoopt tot "Infoplan '91", wordt het informatieplan van Eurotrans bij de directieleden op het bureau bezorgd en vervolgens in de directievergadering toegelicht. En dat blijkt nodig te zijn. De directieleden vragen zich af hoe ze op basis van dit plan een besluit moeten nemen, dat ertoe zal leiden dat de informatievoorziening binnen Eurotrans beter wordt beheerst. De uitgebreide proces- en gegevensanalyses, C/U-matrices, etc. zijn volkomen on(be)grijpbaar voor het management. Een duidelijk overzicht van de kosten en baten van de verschillende projecten ontbreekt. Uiteindelijk besluit de directie toch maar over te gaan tot de realisatie van drie projecten die in het plan zijn beschreven.

Begin 1992 informeert de directie bij de automatiseringsafdeling naar de voortgang van de drie projecten. "Alles loopt op rolletjes", krijgt men te horen. Alleen zal het wat langer duren en wat meer kosten dan gepland, omdat de gebruikersorganisatie niet echt meewerkt.

Tijdens een informele lunch met één van de afdelingshoofden krijgt een directielid te horen dat het helemaal niet op rolletjes loopt. Er is een groot conflict ontstaan tussen de gebruikersorganisatie en de automatiseringsafdeling. Verwijten vliegen over en weer en de projecten lopen helemaal uit de hand. Na spoedoverleg besluit de directie de projecten stil te leggen en de hele zaak nauwkeurig te bestuderen.

Conclusie is dat het informatieplan:
- inmiddels verouderd is;
- niet aansluit op de eisen en wensen van de gebruikersorganisatie;
- geen aandacht aan de technische haalbaarheid heeft besteed.

Omdat het management van Eurotrans onvoldoende zicht heeft op de kwaliteit van de IVP'en wordt voorgesteld de in de vorige paragraaf gepresenteerde management-aanpak te volgen om te komen tot een betere beheersing van de informatievoorziening binnen Eurotrans. In de volgende subparagrafen wordt de management-aanpak stapsgewijs uitgewerkt en toegelicht aan de hand van het voorbeeld.

#### Het vastleggen van doelstellingen van de informatievoorziening
*(Stap 1)*

De hele transportbranche waar Eurotrans in opereert is sterk in beweging. Het is voor Eurotrans dan ook van belang in te spelen op de behoeften van de leveranciers en klanten, teneinde de concurrentie te kunnen volgen en eventueel een voorsprong te nemen. Daarbij is een goede (geautomatiseerde) informatievoorziening onmisbaar.
De informatievoorziening dient daarom het verkoopproces en het logistieke proces zodanig te ondersteunen dat:
- Eurotrans voldoende snel kan reageren op transportopdrachten;
- een goede informatieverstrekking naar klanten is gewaarborgd;
- een goede transportplanning mogelijk is.

Daarnaast dient, gezien de lage marges, een goede financiële afhandeling van de transportopdrachten te zijn gewaarborgd.

#### Het afbakenen van kritieke IVP'en
*(Stap 2)*

Voor de afbakening dienen de IVP'en van Eurotrans te worden gerelateerd aan de doelstellingen van de informatievoorziening (stap 1). Gezien de beperkte omvang van het voorbeeld worden niet alle IVP'en binnen Eurotrans beschreven. Door het cruciale belang van het verkoopproces en het logistieke proces vormen de IVP'en ten aanzien van deze processen de kritieke IVP'en voor Eurotrans. De realisatie van de doelstellingen uit stap 1 is namelijk sterk afhankelijk van de mate waarin de doelstellingen van de IVP'en van het verkoop- en logistieke proces worden gerealiseerd.

**Het ontwikkelen van een stelsel van meetpunten en normen**
*(Stap 3)*

Deze stap geeft aan hoe de meetpunten voor de kritieke IVP'en kunnen worden opgesteld. Voor de eenvoud worden alleen de meetpunten voor de IVP'en ten aanzien van het verkoopproces beschreven.
Bij de beschrijving van het beheersingsvraagstuk is aangegeven dat voor een goede beheersing rekening dient te worden gehouden met alle deelprocessen van de informatievoorziening. In dit voorbeeld worden de meetpunten opgesteld voor de deelprocessen exploiteren/beheren en plannen van de informatievoorziening. Afhankelijk van de resultaten van de stappen 1 en 2 zal de management-aanpak in de praktijk voor alle deelprocessen van de kritieke IVP'en dienen te worden uitgewerkt.

In de vorige paragraaf is al aangegeven dat de voor het management belangrijke meetpunten ten aanzien van de informatievoorziening worden gevonden door de kwaliteitseisen (effectiviteit en efficiëntie) te vertalen naar kwaliteitsattributen en vervolgens naar concrete prestatie-indicatoren. Hierna is voor de deelprocessen exploiteren/beheren en plannen van de IVP'en aangegeven hoe een dergelijke vertaling tot stand komt.

*Exploiteren/beheren van de IVP'en*
Omdat Eurotrans snel en foutloos moet reageren op transportopdrachten en het zich bovendien niet kan veroorloven dat er fouten in de facturen voorkomen, is de betrouwbaarheid van de IVP'en van groot belang. Daarnaast is een goede informatieverstrekking aan klanten en het verkoop-management zeer belangrijk. De informatievoorziening aan de functionarissen van de verkoopafdeling inclusief het management dient, voor een adequate uitvoering van hun functies, goed aan te sluiten bij hun informatiebehoeften.

*Plannen van de IVP'en*
Uit het voorbeeld blijkt dat het proces van informatieplanning niet naar behoren functioneert. Om de effectiviteit van het planningsproces te garanderen dient het informatieplan aan te sluiten op de organisatie, de overige beleidsplannen en het systeemontwikkelproces (analyseren en ontwerpen).

**Het uitvoeren van periodieke metingen**
*(Stap 4)*

Aan de hand van de prestatie-indicatoren dienen periodieke metingen te worden uitgevoerd. Door de metingen per prestatie-indicator te vergelijken met de norm verkrijgt het management inzicht in de kwaliteit van de kritieke IVP'en en de plaatsen waar de kwaliteit van deze processen dient te worden verbeterd. Zo kan uit een meting van één van de prestatie-indicatoren blijken dat het aantal onjuist ingevoerde/verwerkte facturen dertien per week bedraagt (zie figuur 3). Aangezien dit hoger is dan de norm (maximaal tien per week) duidt dit op een te lage kwaliteit.

Kwaliteit van het exploiteren van de IVP'en ten aanzien van het verkoopproces
- Effectiviteit IVP'en ten aanzien van het verkoopproces
  - Betrouwbaarheid IVP'en ten aanzien van het verkoopproces
    - aantal verkooporders dat onjuist wordt ingevoerd/verwerkt
      *Norm: max. 10 per week*
      *max. 4% totaal verkooporders*
    - aantal verkooporders dat te laat wordt ingevoerd/verwerkt
    - aantal fouten in de orderbevestiging, factuur, enz.
    - aantal te laat verwerkte orderbevestigingen, facturen, enz.
    - aantal klachten van klanten over orderbevestigingen, facturen, enz.
  - Mate waarin de opgeleverde informatie voldoet aan de behoefte van het verkoopproces
    - mate waarin IVP'en de functies binnen het verkoopproces ondersteunen
    - tevredenheid verkoopafdeling over de output (op papier en op scherm)
    - aantal klachten afdeling Verkoop over de informatievoorziening
    - aantal klachten van klanten over de informatieverstrekking met betrekking tot transportopdrachten
    - tevredenheid verkoop-management over de management-informatie
- Efficiëntie IVP'en ten aanzien van het verkoopproces
  - ...

*Figuur 3. Meetpunten (en normen) ten aanzien van het exploitatieproces.*

*Figuur 4. Meetpunten ten aanzien van het planningsproces.*

Kwaliteit van het plannen van de informatievoorziening
- Het plannen dient effectief te zijn
  - Informatieplanning dient een informatieplan op te leveren dat goed is afgestemd op de organisatie
    - % afdekking organisatie door informatieplan
    - leeftijd van informatieplan
    - actualiteit van informatieplan
    - aantal keer IT op agenda topmanagement
    - aantal aanpassingen in het informatieplan
    - enz.
  - Informatieplanning dient een informatieplan op te leveren dat goed is afgestemd op de overige beleidsplannen
  - Informatieplanning dient een informatieplan op te leveren dat goed is afgestemd op de operationalisering van het plan (realisatie)
- Het plan dient efficiënt te zijn
  - ...

Bij de periodieke toetsing van de kwaliteit van de kritieke IVP'en kan ter ondersteuning gebruik worden gemaakt van een geautomatiseerd hulpmiddel, zoals een spreadsheet-programma.

**Doorvoeren van verbeteringen in de beheersingsaanpak**
*(Stap 5)*

Door de oorzaken van de afwijkingen tussen de gewenste kwaliteit en de werkelijke kwaliteit te analyseren kan het management van Eurotrans de beheersingsaanpak ten aanzien van de IVP'en verbeteren. Het management kan beslissen om nieuwe beheersingsmiddelen te introduceren, de toepassing van gebruikte beheersingsmiddelen aan te passen of deze niet meer te gebruiken. Aan de hand van het in stap 4 gegeven voorbeeld zou het management kunnen beslissen een betere procedure op te stellen voor het vastleggen van factuurgegevens of meerdere geprogrammeerde controles in het verkoopsysteem op te nemen.

Het resultaat van de management-aanpak is een verbeterde beheersingsaanpak ten aanzien van de voor Eurotrans kritieke IVP'en.

## MANAGEMENT-ONDERSTEUNING

Om voldoende grip te houden op de kwaliteit van de kritieke IVP'en kan het management de hiervoor beschreven aanpak toepassen. Veelal zal het management daarbij behoefte hebben aan ondersteuning van deskundigen op dit gebied. Met name bij het opstellen van het stelsel meetpunten en normen en het samenstellen en eventueel aanpassen van het instrumentarium van beheersingsmiddelen zal de ondersteuning van interne of externe deskundigen wenselijk zijn.

Indien het management daarnaast (periodiek) een onafhankelijk oordeel wil over de kwaliteit van de IVP'en of de beheersing van de informatievoorziening kan het een audit laten uitvoeren door een onafhankelijke en deskundige derde. Juist een EDP-auditor kan door zijn kennis, ervaring en onafhankelijke positie komen tot een dergelijke oordeelsvorming. Hij kan het management daarbij antwoord geven op vragen als:
- Wordt de kwaliteit van de kritieke IVP'en in voldoende mate beheerst?
- Richt de management-aanpak zich op de juiste aandachtsgebieden?
- Worden de beheersingsmiddelen effectief en efficiënt ingezet?

## CONCLUSIE

Door een toegenomen afhankelijkheid van organisaties van de geautomatiseerde informatievoorziening is de kwaliteitsbeheersing van deze informatievoorziening een belangrijk aandachtsgebied voor het management geworden. Als gevolg hiervan wordt het (lijn)management tevens verantwoordelijk gesteld voor de kwaliteit van de informatievoorziening binnen de organisatie. In de praktijk blijkt dit management zijn verantwoordelijkheden nog onvoldoende te dragen. Vaak ontbreekt het aan management-instrumenten om grip te krijgen en te houden op de kwaliteit van de informatievoorziening binnen de organisatie. Dit artikel presenteert een aanpak waarmee het management grip kan krijgen op de kwaliteitsbeheersing van de (geautomatiseerde) informatievoorziening. Het uitgangspunt voor deze aanpak is de doelstelling van de informatievoorziening. Daarnaast is het belangrijk dat het management bij de beheersing rekening houdt met de kritieke delen van de (geautomatiseerde) informatievoorziening.
Met behulp van deze management-aanpak en opgedane ervaringen dient het management in staat te zijn tot een goede kwaliteitsbeheersing van de (geautomatiseerde) informatievoorziening te komen. Een kwaliteitsbeheersing die zeker in de nabije toekomst voor veel organisaties nodig zal zijn om te kunnen overleven.

## LITERATUUR

[Dele90] G.P.A.J. Delen en D.B.B. Rijsenbrij, *Kwaliteitsattributen van automatiseringsprojecten en informatiesystemen*, Informatie jaargang 32 nr. 1, 1990.

[Grev89] N.J.W. Greveling en C.J.T.M. Kokke, *De veranderende betekenis van informatietechnologie voor organisaties*, Informatie jaargang 31 nr. 9, 1989.

[Hops92] B.A.A. Hopstaken en A. Kranendonk, *Informatieplanning; puzzelen met beleid en plan*, tweede herziene druk, Stenfert Kroese, 1991.

[Moon91] H.B. Moonen RA, *Kwaliteitsnormen bij EDP auditing: een kritische beschouwing*, Inaugurele rede prof. H.B. Moonen, 27 september 1991.

[NGI88] NGI, Studierapport *EDP Audit Standaarden*, congres 28 november 1988, NGI sectie EDP Auditing en de EDP Auditors Association Benelux Chapter, 1988.

[NNI80] Nederlands Normalisatie Instituut: NEN 2646, *Kwaliteitsborging. Algemene voorwaarden te stellen voor kwaliteitssystemen voor het ontwerpen, produceren en leveren van produkten en diensten en voor het toepassen van processen*, Delft 1980.

*Drs. G.C.M. Mol*
*Is sinds 1990 werkzaam bij KPMG Klynveld EDP Auditors. Hij heeft zijn studie Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant (KUB) in 1990 afgerond en volgt momenteel de post-doctorale opleiding Accountancy, tevens aan de KUB. Hij heeft met name ervaring op het gebied van administratieve organisatie en kwaliteitsbeheersing.*

*Drs. J.F.H. Vrins*
*Na voltooiing van zijn studie Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant is hij in 1991 als organisatie-adviseur in dienst getreden bij KPMG Klynveld Management Consultants. Hij is onder andere betrokken bij adviesopdrachten op het gebied van informatieplanning, administratieve organisatie en systeemontwikkeling.*

# EDP AUDITORIUM

## NOREA

*9 oktober 1992:*
***Eerste Algemene Ledenvergadering NOREA en Symposium "Trends in Informatietechnologie; trends voor EDP-auditing?"***

*Mw. mr. A.M.Ch. Kemna MBA*

Zoals het voor jonge ouders een hele opgave kan zijn om je kind zo op te voeden dat alle latente talenten tot volle bloei kunnen komen, zo is het voor het bestuur van de NOREA een taak de juiste onderwerpen te kiezen voor haar jaardagen, als één van de middelen om de NOREA zich tot een voor haar leden functionele en nuttige organisatie te laten ontpoppen. En om nog maar even in de ouders/kind-beeldspraak te blijven, zoals gretig door alle sprekers gehanteerd op het oprichtingssymposium van de NOREA: waar kun je als ouder beter mee beginnen dan je kind alle dingen des levens te laten zien waar het specifiek in een vroegtijdig stadium mee geconfronteerd zal worden. Zo zal de NOREA voorop moeten lopen als het gaat om het als beroepsorganisatie inspelen op nieuwe ontwikkelingen in de informatietechnologie. Het onderzoeken of en zo ja, welke invloeden deze ontwikkelingen op het vakgebied EDP-auditing hebben, is dan ook gekozen als onderwerp van het symposium dat de NOREA op 9 oktober 1992 organiseert in de kleine zaal van de Doelen te Rotterdam.

Tijdens het oprichtingssymposium en in de begeleidende symposiumuitgave werd reeds enige keren ingegaan op de mogelijke rol van de EDP-auditor bij ontwikkelingen in en om de informatietechnologie. Zo zag minister Hirsch Ballin in zijn openingsspeech een duidelijke rol weggelegd voor EDP-auditors én accountants bij de bestrijding van een groeiend probleem in onze "vernetwerkende" samenleving: de computercriminaliteit. En prof.dr.ir. Nielen schreef onder meer dat de "NOREAnten" als kwaliteitsingenieurs een zelfstandige rol dienen te spelen bij de controle op de gewenste kwaliteit van coherente systemen: open clusters van gespecialiseerde, kleine systemen, waarin oude en nieuwe, eigen en verworven, van verschillende makelij, samenwerken. Dé trend in informatietechnologie, volgens Nielen.
Het onderwerp voor het symposium van 9 oktober aanstaande komt derhalve niet uit de lucht vallen.

### Ledenvergadering

Het ochtendprogramma zal bestaan uit de eerste Algemene Ledenvergadering van de NOREA, gevolgd door een discussie over een actueel onderwerp binnen het vakgebied. Dit betreft de relatie van de EDP-auditor met de wetgeving. Het ochtendprogramma is uitsluitend toegankelijk voor leden van de NOREA.

### Symposium

's Middags vindt het symposium plaats, dat voor een ieder toegankelijk is. De middag begint met een praktische en theoretische behandeling van de huidige trends in de informatietechnologie. Vragen als welke ontwikkelingen zijn te onderkennen, welke gevolgen hebben deze en wat zijn de verdere toekomstverwachtingen, zullen de revue passeren. Deze professionele kijk in de keuken van de informatietechnologie zal door prof. Martin Healey worden verzorgd. Healey is vice-president van The Institute for Data Processing en directeur van het consultantsbureau Technology Concepts.

Na de behandeling van de trends in de informatietechnologie zal prof.drs. H.C. Kocks RE RA, hoogleraar EDP-auditing aan de Erasmus Universiteit te Rotterdam, de taak op zich nemen de onderkende ontwikkelingen kritisch tegen het licht te houden. Wat betekenen ze voor de EDP-auditor? Betekenen deze trends een verandering in de beheersing van de informatietechnologie? Wat zijn de implicaties voor de audit-praktijk? Zal de EDP-auditor zijn aanpak moeten wijzigen?

Het middagprogramma wordt afgesloten met een paneldiscussie, waarbij de aanwezigen in staat worden gesteld vragen te stellen aan de leden van het panel. Dit panel zal bestaan uit de beide sprekers van het middagprogramma, alsmede de hoogleraren EDP-auditing prof. H.B. Moonen RE RA van de Katholieke Universiteit Brabant, en prof. dr.ir. R. Paans RE en prof.drs. H. de Lange RE RA, beiden van de Vrije Universiteit te Amster-dam. Het symposium zal worden beëindigd met een receptie.

Nadere informatie met betrekking tot de eerste Algemene Ledenvergadering van de NOREA en aansluitend het symposium "Trends in informatietechnologie; trends voor EDP-auditing?" op 9 oktober 1992 in de Doelen in Rotterdam, kunt u verkrijgen bij het secretariaat van de NOREA,
contactpersoon de heer A.J.M. Werring,
A.J. Ernststraat 55,
1083 GR Amsterdam,
telefoon 020 - 6 46 41 99.

## EDP-AUDIT IN NEDERLAND

*Drs. R.Ch.T. Ewals*

### Inleiding

KPMG Klynveld EDP Auditors heeft onlangs een kort onderzoek ingesteld naar EDP-audit-afdelin-

gen in Nederland. Alhoewel het onderzoek door de zeer beperkte doorlooptijd slechts een globaal karakter had, lijkt het zinvol de verkregen resultaten te melden. Doelstelling van het onderzoek was inzicht te verkrijgen in de omvang en aard van de werkzaamheden van EDP-audit-afdelingen in Nederland.

### Aanpak van het onderzoek

Om in een korte tijdsperiode relatief veel gegevens te kunnen verzamelen is bij uitstek de telefonische enquête geschikt [Dekk87]. Eén van de voordelen zijn de hoge responscijfers die telefonische enquêtes gewoonlijk opleveren. De gevraagde informatie dient daarbij zoveel mogelijk in 'top of the mind' van de respondent aanwezig te zijn. Daarnaast moet de gebruikte terminologie aansluiten bij het referentiekader van de respondent.

Om de antwoorden te verkrijgen werd telefonisch contact gezocht met hoofden of medewerkers EDP-audit en IAD van grote ondernemingen in Nederland.

### Beperkingen van het onderzoek

Als gevolg van de korte tijdsperiode waarin het onderzoek kon worden uitgevoerd, moesten beperkingen worden gesteld aan het onderzoek. Hierdoor dienen de onderzoeksresultaten met de nodige voorzichtigheid te worden beschouwd. Enkele aspecten die van belang zijn om de onderzoeksresultaten op hun waarde te kunnen beoordelen zijn:

*Gevoelsmatige antwoorden*
De antwoorden die werden gegeven, berustten vaak op de indruk van de respondent, niet op bekend cijfermateriaal.

*Representativiteit van het onderzoek*
De selectie van ondernemingen heeft niet plaatsgevonden op basis van bekende statistische methoden. Het onderzoek is hierdoor niet noodzakelijkerwijs representatief voor de situatie in heel Nederland.

*Definities*
Voor een aantal gehanteerde begrippen, zoals EDP- auditor, preventief en repressief, bestaan verschillende opvattingen ten aanzien van de betekenis en inhoud van deze begrippen. Hoewel getracht is aan te geven wat algemeen de betekenis is van deze begrippen, bestaat de mogelijkheid dat door respondenten een andere inhoud aan begrippen wordt gegeven. Dit kan, met name gelet op de beperkte omvang van het onderzoek, leiden tot vertekening in de resultaten.

De resultaten van dit onderzoek zullen dan ook niet moeten worden opgevat als normenstellend. Wel kan worden gesteld dat het onderzoek minstens indicatief is en wellicht richtinggevend.

### Onderzoeksresultaten

Het onderzoek heeft een aantal verhoudingscijfers opgeleverd. Onderstaande tabel geeft de gemiddelde waarden weer van de belangrijkste verhoudingsgetallen.

| | Overall | Industrie | Financiële sector | Overheid |
|---|---|---|---|---|
| Aantal EDP-auditors | 8 | 4,5 | 8,5 | 12,5 |
| EDP-auditor : IAD | 1 : 6 | 1 : 7 | 1 : 7 | 1 : 5 |
| EDP-auditor : SO | 1 : 37 | 1 : 67 | 1 : 25 | 1 : 37 |
| EDP-auditor : VTO | 1 : 24 | 1 : 37 | 1 : 17 | 1 : 28 |
| EDP-auditor : automatisering | 1 : 61 | 1 :104 | 1 : 42 | 1 : 64 |
| Preventief : repressief audit | 36 : 64 | 24 : 86 | 50 : 50 | 33 : 67 |
| Preventief : repressief IAD | 28 : 72 | 16 : 84 | 43 : 57 | 23 : 77 |

De resultaten van het onderzoek omvatten de gegevens van twintig ondernemingen in Nederland. Ten behoeve van de resultaten zijn deze ondernemingen onderverdeeld in drie categorieën: de industriële sector, de financiële sector en overheidsinstellingen. De industriële sector omvat zowel handelsbedrijven als bedrijven met een technisch omzettingsproces en de financiële sector zowel banken als verzekeringsinstellingen. De overheidsinstellingen bevonden zich op het niveau van de rijksoverheid.

Van de benaderde ondernemingen was slechts één onderneming niet bereid enige gegevens te verstrekken en bleek één onderneming niet over een IAD en EDP-audit-afdeling te beschikken. De verdeling naar de drie onderscheiden sectoren is als volgt: acht ondernemingen uit de industriële sector, negen ondernemingen uit de financiële sector en drie overheidsinstellingen.

Gemiddeld zijn bij ondernemingen acht EDP-auditors in dienst. Er is echter één onderneming die geen 'echte' EDP-auditors in dienst heeft, maar waarbij de IAD werkzaamheden uitvoert die op het terrein van EDP-auditing liggen. Het maximum aantal EDP-auditors bij één onderneming in dit onderzoek bedraagt 21.[1]

In de literatuur zijn enkele vuistregels aanwezig om het aantal benodigde EDP-auditors in een onderneming te bepalen aan de hand van het totaal aantal automatiseringsmedewerkers [Berg91]. Voor ondernemingen met een automatiseringsafdeling met meer dan 400 medewerkers geldt een vuistregel van 1 EDP-auditor op 40 à 50 automatiseringsmedewerkers. Voor ondernemingen met een automatiseringsafdeling van 40 tot 400 medewerkers geldt een verhoudingsgetal van 1 : 20 à 30. Voor nog kleinere automatiseringsafdelingen geldt een verhoudingsgetal van 1 : 10 à 20. Daarnaast wordt als aanvullende vuistregel een verhouding van 1 EDP-auditor op 10 ontwikkelaars genoemd.

De resultaten van deze enquête geven echter aan dat het hiervoor genoemde verhoudingsgetal van 1 : 10 met betrekking tot het aantal ontwikkelaars

1. *Het aantal EDP-auditors werd bepaald door alle medewerkers op een afdeling die uitvoerende werkzaamheden verrichten op het terrein EDP-auditing hierin mee te nemen, zodat ook zogenaamde 'assistent' EDP-auditors zijn meegeteld. De cijfers betreffen bezettingen per manjaar. Eventuele stagiaires van universiteiten en hogescholen zijn meegenomen in de bemanning indien zij gedurende een substantiële tijd (meer dan een half jaar) een audit uitvoeren.*

PC-beveiliging in een netwerkstructuur
*J.L. Ramos Najera*

Detectie en bestrijding van computervirussen
*J. Brinkman*

The PC as a secure network workstation
*dr. I.G. Graham en S.H. Wieten*

The implementation of TSS
*drs. T.P. de Vries*

### 3 18e jaargang 91/3 herfst 1991

Beveiligingsbeleid geautomatiseerde informatievoorziening
*mw. D. Jansen Heijtmajer*

Geautomatiseerde produktiebesturing
*E.J.M. Ridderbeekx*

Audit van CA-SEVEN
*E.J.M. Ridderbeekx*

Registratie en analyse van produktieproblemen
*ing. J.R. Hendriks en drs. J. Kuipers RA*

SAP en de beheersing van geautomatiseerde controles
*A.A.J. Breed RI, M. Groesz RI en drs. M.A. Weverink*

### 4 18e jaargang 91/4 winter 1991

Systemen voor logische toegangsbeveiliging
*drs. P. Veltman RA*

Toepassing van CA-ACF2 in de praktijk
*ing. D.J. Huis*

Access control op Unisys A Serie computers
*drs. M.A. Bongers RA en J-M. van Leerdam*

Beveiliging van Tandem-systemen
*K.E.A. van Dijk en M.M.J.A. van Dijk*

RACF als access control software voor MVS-omgevingen
*ing. G.H.M. Meijer*

Implementatie van een beveiligingspakket
*J.H. Diekema*

### 1 19e jaargang 92/1 lente 1992

Fysieke beveiliging, een overzicht
*J.F.C. van Epen CISA*

Water en vuur. Effectiviteit van brandbeveiligingsmaatregelen in en om rekencentra
*ing. J.F. Kuperus en ing. G.H.M. Meijer*

Netconditionering
*R. van de Wouw*

Fysieke beveiliging en de chipcard-technologie
*Drs. Th.H. van Hesteren, ing. J.A.M. van Schaik en drs. T.P. de Vries*

Beveiligingsbeleid gegevens en gegevensverwerking, een praktisch voorbeeld
*ir. B.J.M. van Wely*

Forensische EDP-auditing. De rol van de registeraccountant/EDP-auditor bij de bestrijding van computermisbruik
*R.A. s'Jacob RA*

### 2 19e jaargang 92/2 zomer 1992

Investeren in informatietechnologie: take IT or leave IT
*drs.ing. G.J.P. Swinkels en drs. H.G.P. van Irsel*

Managing with Information Technology - a decade of wasted money?
*ir. M.C.A. van Nievelt*

Informatietechnologie in een kantooromgeving: produktiviteitsmanagement van kantoorarbeid en kantoorautomatisering
*drs. F.R.E. Lekanne Deprez*

Het plannen en rechtvaardigen van infrastructurele IT-investeringen
*drs. H.G.P. van Irsel en P. Fluitsma*

Uitbesteding van automatisering: more than make or buy
*mw. drs. H.W.A. van den Heuvel en mw. mr. A.M.Ch. Kemna MBA*