

# De problematiek van de interne controle bij end-user computing

**Drs. D.J. Bais, Drs. F.A.J. Hilhorst en  
Dr. A.H.M. Schrama**

## 1 Inleiding

In het begin van de jaren tachtig deed een nieuw verschijnsel zijn intrede in de automatiseringswereld. Was het maken van computerprogramma's voor die tijd louter voorbehouden aan specialisten, sinds het begin van de jaren tachtig worden ook applicaties geheel of grotendeels door de gebruiker zelf ontwikkeld. Men duidde dit verschijnsel aan als end-user computing (hierna te noemen EUC).

Er zijn hoofdzakelijk twee factoren aan te wijzen, die tot het verschijnsel EUC hebben geleid:

- Ten eerste is in veel organisaties de capaciteit van de automatiseringsafdeling ontoereikend om effectief te kunnen inspelen op de al maar groter wordende vraag van gebruikers naar nieuwe informatiesystemen en naar wijzigingen in bestaande informatiesystemen.
- Ten tweede hebben zich belangrijke ontwikkelingen op het gebied van hard- en software voorgedaan. De ontwikkeltools en standaardpakketten die op de markt kwamen werden steeds krachtiger en meer gebruikersvriendelijk. Daarnaast nam ook de bekendheid met de computertechnologie in brede lagen van de bevolking toe, mede als gevolg van de prijsdaling van de personal computer (pc).<sup>1</sup>

EUC beperkt zich echter niet alleen meer tot het gebruik van pc-toepassingen. Door het beschikbaar komen van meer gebruikersvriendelijke software voor het mainframe is ook deze apparatuur binnen het bereik van end-users gekomen. Niet meer alleen professionele automatiseringsafdelingen zijn in staat

computerprogramma's te ontwikkelen. Met behulp van 4e generatie softwaretools is dit nu ook mogelijk voor gebruikersafdelingen.<sup>2</sup> Echter een risico daarvan is dat binnen de organisatie geen afstemming plaatsvindt en dat de uitwisselbaarheid van de produkten van deze informatiesystemen gering of niet aanwezig is. Bij traditionele vormen van systeemontwikkeling vindt sturing van bovenaf plaats. EUC daarentegen speelt zich op initiatief van de gebruiker aan de basis van de organisatie af. Voordelen van EUC zijn dat het zelfstandigheid en flexibiliteit biedt en dat voor zover EUC met behulp van de pc plaatsvindt, geautomatiseerde gegevensverwerking ook binnen het bereik van kleinere organisaties is gekomen. Daartegenover staat dat EUC nadelige gevolgen kan hebben voor de administratieve organisatie en het daarmee verband houdende stelsel van interne controle. EUC brengt op centraal niveau in de organisatie als gevolg hiervan een coördinatie- en beheersingsproblematiek met zich mee.<sup>3</sup> Op deze laatste aspecten van EUC zullen wij ons in dit artikel vooral richten.

Drs. D.J. Bais, heeft Economie (1975) en Bestuurlijke Informatiekunde (1989) gestudeerd aan de UvA. Hij is achtereenvolgens werkzaam geweest bij overheid, onderwijs en het GAK. Hij is thans werkzaam bij de Nederlandsche Bank. Dit artikel is geschreven a titre personnel.

Drs. F.A.J. Hilhorst, heeft Bestuurlijke Informatiekunde gestudeerd aan de UvA (1989). Vóór dit artikel was afgerond is hij geëmigreerd naar de Verenigde Staten.

Dr. A.H.M. Schrama, is na het behalen van het doctoraat in de wiskunde en natuurwetenschappen (1973) verbonden geweest aan het Gemeentelijk centrum voor Elektronische Informatieverwerking te Amsterdam. Sinds 1976 is hij als hoofddocent verbonden aan de vakgroep Bestuurlijke Informatiekunde van de UvA. Hij publiceerde in 1989 een boek over persoonlijk computergebruik.

De *coördinatieproblematiek* bestaat met name hierin, dat men er zorg voor dient te dragen, dat de activiteiten van alle binnen de organisatie te onderscheiden subsystemen optimaal afgestemd blijven op het realiseren van de doelstellingen van de organisatie als geheel. Bij EUC is dit echter vanwege het ontbreken van inzicht in ontwikkelingen die in de organisatie plaatsvinden niet altijd mogelijk.

De *beheersingsproblematiek* bestaat met name hierin dat EUC de neiging heeft te leiden tot een erosie van het stelsel van interne controle. Deze erosie wordt door de volgende eigenschappen in de hand gewerkt:

- Ten eerste vindt er bij EUC bij het ontwikkelen van informatiesystemen over het algemeen geen functiescheiding plaats tussen de ontwikkelaars, de beheerders en de gebruikers van het systeem. Daarnaast worden meestal geen gestructureerde systeemontwikkelingsmethoden en -technieken toegepast.
- Automatisering leidt vrijwel altijd tot een herverdeling en reallocatie van taken en functies en brengt daarmee verandering aan in de bestaande organisatiestructuur. In belangrijke mate zal dit ook het geval zijn bij EUC. Echter waar bij traditionele vormen van automatisering deze veranderingen doorgaans van bovenaf gepland en gecoördineerd worden zal dit bij EUC minder het geval zijn.
- Een EUC-systeem zal veelal het karakter hebben van een ad-hoc respons op een informatiebehoefte. Het opzetten en bijhouden van documentatie wordt verwaarloosd. Men heeft de neiging om een korte-termijnbril op te zetten. Bovendien zal deze subjectieve urgentie er op lokaal niveau in de organisatie toe leiden dat men de voorgenomen EUC-activiteit zoveel mogelijk aan het centrale coördinatie- en beheersingsmechanisme zal willen onttrekken.

Om deze problematiek in kaart te brengen is door ons een literatuurstudie en een veldonderzoek verricht. Over interne controle in relatie tot EUC bestaat echter betrekkelijk weinig literatuur. Het veldonderzoek bestond uit een aantal interviews met deskundigen op dit gebied. Daarnaast zijn eigen ervaringen verdisconteerd. Achtereenvolgens komen in de volgende paragrafen aan de orde: de eigen-

schappen en de daarmee samenhangende risico's van EUC, maatregelen die tegen deze risico's getroffen kunnen worden en de conclusies.

## 2 De eigenschappen van EUC

Alvorens in te gaan op de eigenschappen van EUC zullen we hier eerst een nadere begripsbepaling van EUC dienen vast te stellen. Omdat de term 'End-user computing' aan de praktijk is ontsproten is er niet zoiets als een algemeen aanvaarde definitie van EUC. In de literatuur ziet men dan ook, dat er verschillende interpretaties bestaan van het begrip EUC. Om verwarring bij het lezen van dit artikel te voorkomen geven wij hier onze definitie van EUC: *EUC is iedere vorm van geautomatiseerde gegevensverwerking waarbij gebruik wordt gemaakt van een applicatie, die door de gebruiker in zijn eigen werkomgeving ontwikkeld is.*

Uit deze definitie kunnen drie kenmerken afgeleid worden aan de hand waarvan we een EUC-applicatie kunnen onderscheiden van een 'gewone' applicatie:

- Er moet daadwerkelijk sprake zijn van het zelf ontwikkelen van een applicatie.
- Bij een EUC-applicatie berust de verantwoordelijkheid omtrent de juiste werking van de applicatie en het beheer en gebruik van de applicatie bij een en hetzelfde orgaan in de organisatie.
- Applicatie-ontwikkeling geschiedt in principe in de eigen werkomgeving en onttrekt zich daardoor gemakkelijk aan het stelsel van interne controle in de organisatie.

EUC wordt in de literatuur over het algemeen vereenzelvigd met pc-gebruik. Volgens onze definitie van EUC is dit dus niet terecht.<sup>4</sup> Echter, het is wel zo dat veel EUC zich afspeelt in een pc-omgeving. Bij het behandelen van de interne controleproblematiek van EUC is dan ook, waar dit relevant is, de interne controleproblematiek bij het gebruik van de pc onder de loupe genomen. Om een nader inzicht te verkrijgen in de problematiek van de interne controle bij EUC hebben wij de eigenschappen en de daarmee samenhangende risico's van EUC onderverdeeld in twee hoofdcategorieën, te weten:

*Algemene risico's:* risico's die verband houden met

algemene karakteristieken van een EUC-omgeving.

*Situatie-specifieke risico's:* risico's die naar aard en intensiteit zullen verschillen al naar gelang de specifieke hard- en software-omgeving waarin EUC zich afspeelt. Deze hoofdcategorieën zullen nu in aparte paragrafen worden behandeld.

### 3 Algemene risico's

Allereerst komen de algemene risico's aan de orde. Het probleem bij EUC blijkt te zijn, dat het noodzakelijke niveau van controle en beveiliging dat in een traditionele automatiseringsomgeving wel gerealiseerd kan worden in een EUC-omgeving doorgaans veel moeilijker te realiseren is.<sup>5</sup> Dit komt omdat een EUC-omgeving in het algemeen eigenschappen zal bezitten die de neiging hebben te leiden tot een erosie van het stelsel van interne controle. Het gaat hierbij om de volgende eigenschappen:

*Decentralisatie:* EUC heeft op de gegevensverwerking een decentraliserende invloed.

*Instabiliteit:* EUC heeft op de administratieve organisatie een destabiliserende invloed.

*Vrijheid/zelfstandigheid:* EUC geeft gebruikers vrijheid en zelfstandigheid.

*Korte-termijngerichtheid:* EUC-applicaties worden vrijwel altijd vanuit een korte-termijnoptiek ontwikkeld.

*Verantwoordingsstructuur:* Het is in een EUC-omgeving vaak onvoldoende duidelijk wie verantwoordelijk is voor wat.

*Ervaring:* Gebruikers hebben over het algemeen weinig specifieke ervaring op automatiseringsgebied.

Wij zullen nu de hiervoor genoemde eigenschappen van een EUC-omgeving nader toelichten.

#### *Decentralisatie*

Er bestaat in een organisatie altijd een zeker spanningsveld tussen dat wat men op centraal niveau als efficiënt en optimaal ziet en hoe men dat op decentraal niveau in de organisatie ervaart. Ook bij de informatievoorziening bestaat dit spanningsveld. Dit is een van de drijvende krachten achter het verschijnsel EUC. Centrale informatiesystemen worden in principe altijd van bovenaf ontworpen. Dit kan tot gevolg hebben, dat met bepaalde informatie-

wensen van de gebruikers geen of te weinig rekening wordt gehouden. Ook is het heel goed mogelijk dat de gebruikers bepaalde van bovenaf ingestelde administratieve procedures als inefficiënt en zelfs als hinderlijk ervaren. EUC geeft aan de gebruikers, en dat is een belangrijk voordeel, de werktuigen in handen om zelf wat aan deze on vervulde informatiewensen en de door hen als problematisch ervaren situatie te doen.

EUC stelt de gebruiker aldus in staat om op decentraal niveau hun eigen werkzaamheden anders in te vullen en te organiseren.

#### *Instabiliteit*

Nauw verwant aan de hiervoor beschreven decentralisatietendens is het verschijnsel van de instabiliteit van de administratieve organisatie in een EUC-omgeving. Om een voorbeeld te geven: Stel dat oorspronkelijk bepaalde gegevens worden bijgehouden in de centrale database. Het systeem voldoet niet en wordt daarom aangevuld met een stand-alone EUC-applicatie, waarin gedeeltelijk dezelfde gegevens worden bijgehouden. Na verloop van tijd blijkt echter dat de meest complete, accurate en tijdige versie van deze gegevens niet meer in de centrale database wordt bijgehouden maar op de pc met EUC-applicatie. Andere gebruikers, die van dezelfde gegevens gebruik maken, gaan zich nu hierop instellen en stemmen hun werkzaamheden voortaan af op de EUC-applicatie in plaats van op het centrale informatiesysteem. Het zal duidelijk zijn dat hier sprake is van een niet-gecoördineerde substantiële ingreep in de administratieve organisatie. Wijzigingen in de administratieve organisatie van het hier beschreven type zijn in een EUC-omgeving zeker niet denkbeeldig.

#### *Vrijheid/zelfstandigheid*

EUC levert de gebruiker een nieuw verworven vrijheid en zelfstandigheid op. Deze is nu in staat om een aantal informatieproblemen op een creatieve manier op te lossen, zonder daarbij afhankelijk te zijn van een in zijn ogen traag en log apparaat als de centrale automatiseringsafdeling. Bovendien kan hij het zelf maken van een applicatie als een zeer dankbare en aangename bezigheid ervaren. In deze nieuw verworven vrijheid zal de gebruiker zich niet graag laten beperken. Hij zal dan ook bij het

ontplooiën van zijn EUC-initiatieven zoveel mogelijk zijn eigen gang willen gaan. Het gevolg hiervan is dat de gebruiker de neiging zal hebben om, wanneer dit maar enigszins mogelijk en verdedigbaar is, zijn EUC-activiteiten aan het centrale coördinatie- en beheersingsmechanisme te onttrekken.

#### *Korte-termijngerichtheid*

EUC-applicaties worden ontwikkeld naar aanleiding van een informatieprobleem dat de gebruiker zelf als urgent ervaart. Het gevolg is dat EUC-applicaties vrijwel altijd vanuit een korte-termijnoptiek worden ontwikkeld. Hierbij bestaat de neiging tot het kiezen voor de zogenaamde 'quick and dirty' oplossingen.<sup>6</sup> Daarnaast is het zeer de vraag of de EUC-oplossing wel past binnen de lange-termijnproblemen waarvoor de organisatie zich als geheel gesteld ziet.

#### *Verantwoordingsstructuur*

Het min of meer zelfstandig ontwikkelen van applicaties brengt voor de gebruiker nieuwe verantwoordelijkheden met zich mee. Het gaat hierbij onder meer om:

- beheer van de applicatie;
- het verzorgen van documentatie en het up-to-date houden daarvan;
- het beheer van gegevens;
- het verzorgen voor een adequate back-up.

De gebruikers zullen vanuit hun specifieke gebruikersachtergrond veelal niet gewend zijn om deze verantwoordelijkheden te dragen. Daarnaast zullen zij hiertoe veelal ook niet adequaat zijn opgeleid. Over het algemeen wordt een EUC-omgeving dan ook gekenmerkt door een onduidelijke verantwoordingsstructuur, waarbij niet duidelijk is vastgelegd wie verantwoordelijk is voor wat.

#### *Ervaring*

Hoe mooi de softwaretools ook mogen zijn, die de gebruiker-ontwikkelaar hedentendage ter beschikking staan, zij maken hem daarmee nog niet gelijkwaardig aan een geschoolde automatiseringsdeskundige. EUC-applicaties worden dan ook zelden met behulp van een gestructureerde ontwikkelingsmethode ontwikkeld.<sup>7</sup> Ook worden zij veelal niet adequaat getest voor ingebruikname en zijn zij meestal

slecht gedocumenteerd. Het gevaar is derhalve niet denkbeeldig dat een EUC-applicatie zo op het oog doet wat hij doen moet, maar bij nader inzien toch fouten blijkt te bevatten. Vanwege het ontbreken van een gestructureerde ontwikkelingsmethode en de gebrekkige documentatie, kan het verhelpen van deze fouten een zeer tijdrovende en moeizame aangelegenheid zijn.

Hiervoor hebben wij slechts enige karakteristieken van een EUC-omgeving aangegeven. Niet alle zes genoemde eigenschappen zullen in iedere EUC-omgeving even sterk aanwezig zijn. Echter, bij de beslissing om een te ontwikkelen applicatie al dan niet aan een EUC-omgeving toe te vertrouwen, zal men met de hiervoor beschreven eigenschappen van een EUC-omgeving terdege rekening moeten houden.<sup>8</sup>

#### **4 Situatie-specifieke risico's**

De risico's, die hiernavolgend aan de orde komen, houden primair verband met de hard- en software-omgeving, waarin EUC zich afspeelt. Vandaar dat wij ze situatie-specifieke risico's hebben genoemd. We onderscheiden hierbij risico's bij de volgende omgevingen: mainframe/mini, pc en pc-lan en situaties waarbij interfaces tussen EUC en de centrale computerfaciliteiten bestaan.

Bedacht dient te worden dat tegenover deze risico's belangrijke voordelen van EUC staan. Een pc geeft de gebruiker ervan direct gemak en de vrijheid zelf onafhankelijk van anderen zijn informatiewensen te vervullen. PC-netwerken en up- en downloading kunnen zeer efficiënt zijn en geven de gebruiker directe toegang tot gegevensbestanden, die in eigen applicaties benut kunnen worden.

##### *De mainframe/mini-omgeving*

In de mainframe/mini-omgeving is de technologie en de organisatie van de controle en beveiliging het verst ontwikkeld. In principe kan men deze hardware-omgeving dan ook beschouwen als relatief de meest veilige. Back-up en recovery zijn beter geregeld dan bij pc-applicaties, omdat deze niet onder de paraplumaatregelen van de centrale automatiseringsafdeling vallen.<sup>9</sup> Echter bij EUC stelt men aan de gebruikers ontwikkeltools ter beschikking. Wanneer een gebruiker zich door middel van deze tools

toegang weet te verschaffen tot programma- c.q. gegevensbestanden, die buiten zijn competentiegebied liggen, en daar ongeautoriseerde mutaties weet aan te brengen, kan dit tot aanzienlijke schade leiden. Door middel van toegangsbeveiliging dient er dus een stringente scheiding te worden aangebracht en te worden gehandhaafd tussen de EUC-omgeving en de centrale informatiesystemen. Binnen de EUC-omgeving kan er door middel van het creëren van overdrachtsmomenten een volgtijdelijke scheiding worden aangebracht tussen de productie- en ontwikkelomgeving. Verder dient men de ontwikkeltools die men aanschaft en ter beschikking stelt aan de gebruiker, te beoordelen op hun mogelijk schadelijk penetratievermogen tot in programma- en gegevensbestanden, die behoren tot een competentiegebied, waartoe de gebruiker geen toegang zou mogen krijgen. Pogingen van end-users om zich toegang te verschaffen tot programma's en bestanden, die buiten hun competentiegebied liggen kunnen met behulp van de mogelijkheden (logging) die deze omgeving biedt achterhaald worden.

## *De pc omgeving*

De controle en beveiliging is, ondanks ontwikkelingen met name op het gebied van toegangsbeveiliging, nog van een lager niveau dan in de mainframe-omgeving. Er zijn dan ook afhankelijk van de belangrijkheid van de applicatie risico's verbonden aan EUC in een pc c.q. pc-lan-omgeving. Deze risico's houden verband met een tweetal factoren te weten: de aard van het *besturingssysteem* van de pc en de aard van de gegevensdragers, die bij pc-gebruik behoren. De kennis omtrent de werking van het besturingssysteem van de pc is, sinds de pc tot in de huiskamer van vele particulieren is doorgedrongen, wijdverbreid. Wie tot op het besturingsniveau van de pc weet door te dringen kan in principe een vrijwel onbeperkt aantal manipulaties verrichten met alle aanwezige bestanden.

Binnen de huidige staat van de pc-technologie is het vrijwel onmogelijk om de geoefende gebruiker effectief de toegang tot pc-bestanden te ontfemen. Het gevolg hiervan is, dat er geen effectieve scheiding is aan te brengen tussen de ontwikkel- en de productie-omgeving. Daarnaast kan iedere in de applicatie ingebouwde controle, of deze nu gepro-

grammeerd of handmatig geschiedt, door manipulaties op besturingsniveau omzeild worden. Logging staat bij de pc nog in de kinderschoenen. Ongeautoriseerde manipulaties met data en programma's (die overigens lang niet altijd met kwade opzet behoeven te geschieden), zijn dus achteraf vrijwel niet op te sporen.

Verder is het bij de pc praktisch onmogelijk om in een applicatie een audit-trail in te bouwen die niet buiten de applicatie om door de gebruiker beïnvloed kan worden. Meestal bestaat het audit-trail bij een pc-applicatie, zo dit al aanwezig is, alleen uit mutatie- en inleesverslagen. Deze verslagen kunnen vernietigd worden, waarna men ze na het aanbrengen van enige wijzigingen buiten de applicatie om opnieuw afdrukt.

Bij de pc wordt van twee typen gegevensdragers gebruik gemaakt:

- de hard-disk;
- de 'floppy'-disk.

Zowel de hard-disk als de 'floppy'-disk zijn gevoelig voor beschadiging. Er dienen dus regelmatig back-ups gemaakt te worden. De praktijk wijst echter uit, dat de discipline hiertoe (zeker in een EUC-omgeving) veel te wensen overlaat.

Het nut van het maken van back-ups is groter indien bij storingen van herstartpunten gebruik kan worden gemaakt. Het is niet denkbeeldig, dat deze EUC-applicaties zullen ontbreken. Daarnaast kunnen er tussen pc's door middel van 'floppy'-disks gemakkelijk gegevens uitgewisseld worden. Dit heeft belangrijke voordelen, maar in controle-technisch opzicht is het riskant. Privacygevoelige en strategische gegevens kunnen op deze wijze op eenvoudige wijze buiten de organisatie geraken. Aan de andere kant kunnen ongewenste zaken zoals virussen via 'floppy'-disks een organisatie binnenkomen. Wij denken hierbij met name aan privésoftware van werknemers (bijvoorbeeld spelletjes) en aan op de computers van werknemers thuis verrichte werkzaamheden.

## *Pc-lan-omgeving*

De meeste van de hiervoor genoemde risico's voor pc's gaan ook in een lan-omgeving op (lan=local area network).<sup>10</sup> Bij een lan wordt een aantal pc's via datacommunicatielijnen met elkaar verbonden. In het

netwerk kunnen bepaalde pc's centrale functies gaan vervullen. Bijvoorbeeld een pc gaat fungeren als file-server. De gegevensbestanden die in deze pc worden opgeslagen krijgen het karakter van een centrale database. Iedere pc uit het netwerk kan min of meer vrijelijk over deze bestanden beschikken. Voordelen daarvan zijn de toegankelijkheid van de informatie en de efficiency van eenmalige vastlegging. Dit maakt deze centrale database behalve tot een zeer toegankelijke ook tot een zeer kwetsbare. Met een goed systeembeheer zijn deze bezwaren gedeeltelijk te ondervangen. Vanwege het feit, dat meerdere gebruikers met meerdere applicaties van het netwerk gebruik kunnen maken dienen speciale eisen aan de software gesteld te worden. Voorkomen dient te worden dat, doordat gebruikers tegelijkertijd mutaties (simultane update) in de bestanden aanbrengen, zogenaamde dead-locks ontstaan. De applicaties zijn dan niet meer bereikbaar. Als oplossing zetten de gebruikers hun pc's dan uit en aan. Gevolg hiervan kan zijn, dat de integriteit van de bestanden wordt aangetast. Een juist gebruik van pc-netwerken vraagt specialistische kennis. Over het algemeen beschikken end-users hierover niet. Bovendien vraagt het gebruik van netwerken een zeer duidelijke en niet te onderschatten administratieve-organisatorische coördinatie, dit om te voorkomen dat onduidelijkheden gaan ontstaan over de juistheid, volledigheid, recentheid en de locatie van de verschillende databestanden in het netwerk en de verantwoordelijkheid daaromtrent.

### *Interfacing*

Vaak zullen er tussen de centrale informatiesystemen en een EUC-applicatie gegevens uitgewisseld worden. Onder de centrale informatiesystemen verstaan wij hier systemen, die onder het beheer van de centrale automatiseringsafdeling vallen. Het uitwisselen van gegevens kan op drie manieren geschieden:

- 1 Door het handmatig intoetsen van gegevens. Hierbij bestaat er kans op accuratessefouten.
- 2 Door up- en downloading. Zoals eerder gesteld, is de kans dat een EUC-applicatie fouten bevat groter dan bij een volgens gestructureerde methode ontwikkelde en geteste applicatie. Het zal duidelijk zijn, dat wanneer er

via uploading foutieve gegevens naar de centrale database worden overgebracht, dit ook voor de centrale informatiesystemen verstrekken de gevolgen kan hebben. Bij downloading bestaat, naast het voordeel direct en op efficiënte wijze over gegevens te kunnen beschikken, het gevaar dat de gegevens die naar de EUC-omgeving zijn overgebracht verouderen. De EUC-applicatie opereert dan met verouderde gegevens en levert informatie op, die mogelijk verkeerd geïnterpreteerd zal worden. Het aanbrengen van een datumkenmerk op de te downloaden gegevens en het weergeven van dit kenmerk op de door de EUC-applicatie geproduceerde verslagen is noodzakelijk. Wanneer men privacy-gevoelige en strategische gegevens download naar de EUC-omgeving, dient men er zich bewust van te zijn dat deze gegevens van een relatief veilige naar een relatief onveilige omgeving worden overgebracht. Deze gegevens zullen indien noodzakelijk met speciale zorg omgeven dienen te worden. Tenslotte, maar zeker niet op de laatste plaats, moet men zich zowel bij up- als bij downloading bewust zijn van de risico's die optreden wanneer men een pc aansluit op het mainframe c.q. de mini. De pc bezit eigen intelligentie. Met behulp van de pc kan de gebruiker trachten binnen te dringen in programma's en bestanden die buiten zijn competentiegebied liggen. De geoefende gebruiker geeft men hiertoe met de pc als intelligente terminal een bijzonder krachtig werktuig in handen. Men dient bij het aansluiten van pc's op het mainframe c.q. de mini de nodige voorzichtigheid te betrachten en toegangsbeperkende maatregelen te treffen.<sup>1</sup>

- 3 Door het geven van directe toegang tot centrale systemen aan EUC-applicaties.

In principe kan men aan een EUC-applicatie twee vormen van directe toegang verlenen: de EUC-applicatie mag uitsluitend centrale gegevensbestanden lezen en de EUC-applicatie mag lezen en schrijven in centrale gegevensbestanden. Aan beide vormen van directe toegang zijn belangrijke risico's verbonden. Dit zal zeker het geval zijn wanneer de EUC-applicatie zich op de pc bevindt en de centrale gegevensbestanden zich op het mainframe bevinden. Wanneer men aan een EUC-applicatie directe toegang tot het

mainframe verleent, dan zal men feitelijk binnen de EUC-omgeving eenzelfde niveau van controle en beveiliging dienen te realiseren als in het automatiseringscentrum.

## **5 Maatregelen**

Organisaties dienen eisen te stellen aan de met behulp van informatiesystemen gegenereerde informatie. Deze eisen hebben over het algemeen betrekking op kwaliteitsaspecten als de betrouwbaarheid van de informatie, de efficiency waarmee de informatie tot stand komt, de beheersbaarheid en de vertrouwelijkheid van informatiesystemen. EUC heeft, naast een aantal voordelen, eigenschappen die risico's voor deze kwaliteitsaspecten inhouden. In deze paragraaf komen maatregelen aan de orde die tot verkleining van deze risico's kunnen leiden.<sup>12</sup>

Het moge duidelijk zijn dat, alvorens maatregelen worden getroffen, eerst goed naar de aard van het systeem en de aard van de door het systeem verwerkte gegevens moet worden gekeken, anders worden vrij risicoloze systemen met een overmaat van meestal dure controle- en beveiligingsmaatregelen omgeven. De voordelen van EUC kunnen daardoor geheel of gedeeltelijk teniet worden gedaan. In hoofdlijnen behelzen de mogelijke maatregelen het volgende:

### *1 Maatregelen ter bevordering van de betrouwbaarheid van informatie*

- Voorschriften uitvaardigen voor de documentatie van programma's.  
Indien bruikbare documentatie aanwezig is wordt de continuïteit van systemen bevorderd omdat onderhoud gemakkelijker kan plaatsvinden. Dit geldt ook voor de overdraagbaarheid van systemen naar andere afdelingen en bij personeelswisselingen.
- Kritische applicaties niet in een pc-omgeving toestaan.  
Aangezien de pc-omgeving grotere risico's met zich meebrengt is het wenselijk belangrijke applicaties niet in deze omgeving onder te brengen.
- Het voornemen EUC-applicaties te ontwikkelen dient gemeld te worden aan een centraal punt.  
Bij het ontwerpen van EUC-applicaties wordt

veelal onvoldoende rekening gehouden met bestaande organisatorische aspecten.

- De EUC-organisatie van de gegevensverwerking regelmatig doorlichten.  
Hieruit kan bijvoorbeeld blijken dat de kritische aard van de applicatie het noodzakelijk maakt dat (meer) functiescheiding moet worden toegepast.
- Fysieke beveiliging toepassen.  
Teneinde hard- en software te beschermen tegen onbevoegd gebruik en calamiteiten kan het noodzakelijk zijn één en ander in beveiligde ruimten onder te brengen.
- End-users opleiden in het gebruik van gestructureerde ontwikkelingsmethoden.  
Hiermee wordt bevorderd dat applicaties beter gedocumenteerd en getest worden en dat backup en recovery mogelijkheden aanwezig zijn.
- Uploaden van gegevens met restricties omgeven en gegevenscontrole toepassen.  
De kans bestaat dat de te uploaden gegevens gegenereerd zijn door een niet voldoende geteste applicatie en dat aldus onbetrouwbare gegevens in het mainframe komen. Om dit te vermijden kan uploading via een tussenslag met gegevenscontrole plaatsvinden.
- Downloaden van gegevens met restricties omgeven en gegevenscontrole toepassen.  
In de EUC-omgeving worden gegevens niet zelden door middel van niet adequaat geteste en ad-hoc gemaakte applicaties bewerkt. De kans op vervorming van gegevens neemt hierdoor toe. Daarnaast is de kans op veroudering van gegevens aanwezig.
- In een pc-omgeving regels voor diskettebeheer opstellen.  
Dit betreft backup- en bewaarprocedures, omdat ten aanzien hiervan in een pc-omgeving meestal weinig discipline bestaat.
- Uitwijkmogelijkheden regelen.  
Bij calamiteiten kan zodoende de betrouwbaarheid van de informatie in stand blijven.
- De toegang tot kritische applicaties zoveel mogelijk beveiligen. Om te voorkomen dat ongeautoriseerde bewerkingen van gegevens plaatsvindt kan de toegang tot applicaties door een reeks van maatregelen beveiligd worden.  
Genoemd kunnen worden: hardware-matige terminalidentificatie, EUC-faciliteiten centraal be-

heren (software-tools), het instellen van wachtwoorden en het gebruik van chipkaarten.

## 2 Maatregelen ter bevordering van de efficiency

- Overlegstructuren creëren tussen gebruikers (groepen).

Uitwisseling van ervaringen leidt tot een beter product en kan tevens voorkomen worden dat herhaling van fouten optreedt. Door een gebrek aan coördinatie van de administratieve organisatie worden afzonderlijke systemen niet goed op elkaar afgestemd. Dat kan leiden tot beperkingen in de uitwisselbaarheid van gegevens.

- Regelmatig inventarisatie van EUC-activiteiten houden.

Dit kan meervoudige gegevensvastlegging binnen de organisatie verminderen. Bovendien wordt zicht verkregen op de EUC-ontwikkelingen die zich binnen de organisatie voordoen.

- Het laten uitvoeren van kosten- en batenanalyses.

Hierdoor worden overhaaste dan wel onjuiste beslissingen (mede op grond van hobbyisme in een EUC-omgeving) tot het ontwikkelen van nieuwe systemen vermeden.

- Urenverantwoordingen van EUC-activiteiten laten bijhouden.

Ongewenste ontwikkelingen als inefficiënte systeemontwikkeling kunnen hierdoor tijdig gesignaleerd worden.

- End-users opleiden in het gebruik van gestructureerde ontwikkelingsmethoden.

Hiermee wordt een efficiënte systeemontwikkeling bevorderd.

- Selectieprocedures instellen voor hard- en software.

Dit voorkomt dat afstemmingsproblemen ontstaan tussen programmatuur en hardware en dat de hardware niet efficiënt benut wordt.

- Het gebruik van bepaalde hard- en software voorschrijven.

Zonder uniformiteit van hardware en softwarepakketten wordt binnen een organisatie de uitwisselbaarheid van programma's en gegevens belemmerd.

## 3 Maatregelen ter bevordering van de beheersbaarheid van informatiesystemen

- Het regelmatig doorlichten van de administratieve organisatie.

Als gevolg van de dynamiek die in een EUC-omgeving bestaat kunnen ongewenste veranderingen optreden in de gegevensverwerking, bijvoorbeeld de vermindering van functiescheiding of het gebruik van afwijkende hardware.

- Gegevens onder beheer stellen van een eigenaar. Hierdoor wordt duidelijk wie of welke afdeling bepaalde verantwoordelijkheden ten aanzien van systemen en gegevens draagt. Wijzigingen in applicaties dienen gefiatteerd te worden door de eigenaar van de gegevens waarvan de applicatie gebruik maakt.

- De werking van applicaties laten testen door derden. Omdat bij EUC veelal onvoldoende getest wordt dient vastgesteld te worden of de applicatie aan de gestelde eisen voldoet.

- Standaards instellen ten aanzien van systeemontwikkelingsmethoden.

Bij EUC bestaat de neiging tot ad-hoc ontwikkelingen. Als gevolg hiervan kan te veel divergentie in de toegepaste methoden en het systeemgebruik optreden. Dit beperkt de beheersbaarheid van de informatiesystemen in de organisatie.

- End-users trainen in het dragen van verantwoordelijkheden.

End-users zijn zich van hun verantwoordelijkheden ten aanzien het beheer van systemen doorgaans minder bewust.

## 4 Maatregelen ten aanzien van de vertrouwelijkheid van de informatiesystemen

Het risico dat vertrouwelijke informatie uitlekt is, in vergelijking met andere hardware bij het gebruik van pc's groter.

- Downloaden niet of met aanzienlijke beperking toestaan.

Bij downloading worden gegevens vanuit de doorgaans goed beschermde mainframe-omgeving naar de moeilijker te beveiligen pc overgebracht. Bij het downloaden kunnen speciale beveiligingsmaatregelen worden toegepast zoals data-encryptie, modem-beveiliging, hardwarematige terminalidentificatie en het beveiligen van de informatiedragers zoals diskettes.

- Beheerprocedures ten aanzien van diskettes instellen.  
Deze maatregel is ingegeven door het feit dat diskettes gemakkelijk ongezien buiten de invloedssfeer van de organisatie kunnen geraken. Een andere oplossing hiervoor is slechts het gebruik van pc's zonder discdrive voor uitwisselbare diskettes toestaan.

Voor al deze maatregelen geldt dat controle op de naleving ervan, vooral gezien het dynamische en ad-hoc karakter van EUC, noodzakelijk is.

Een oplossing om dit te waarborgen kan zijn dat de hiervoor genoemde maatregelen onderdeel vormen van een algeheel kwaliteitssysteem dat de eisen bevat waaraan het ontwikkelen en gebruik van informatiesystemen in de organisatie moeten voldoen.<sup>13</sup>

## 6 Conclusies

Aan het toepassen van EUC zijn naast voordelen niet te onderschatten risico's verbonden. Tot heden hebben organisaties de toepassing van controle- en beveiligingsmaatregelen voornamelijk gericht op informatiesystemen in een mainframe-omgeving. De te verwachten verdere toename van EUC door het algemeen worden van programmeertools en standaardpakketten impliceert dat tevens de daarmee samenhangende risico's dienen te worden beheerst. De organisatie, die zich van deze risico's niet bewust is, kan voor onaangename verrassingen komen te staan. Voor een deel houden de risico's van EUC verband met algemene eigenschappen van een EUC-omgeving. Deze omgeving wordt door de volgende eigenschappen gekarakteriseerd:

- decentralisatie van de gegevensverwerking;
- het ontstaan van min of meer spontane veranderingen in de administratieve organisatie;
- het onttrekken van de EUC-activiteiten aan het centrale coördinatie- en beheersingsmechanisme;
- korte-termijngerichtheid;
- een doorgaans onduidelijke verantwoordingsstructuur;
- een gebrek aan automatiseringservaring bij de gebruikers.

Daarnaast is er nog een aantal specifieke factoren van belang, zoals de hardware-omgeving waarin

EUC zich afspeelt, de software die daarbij benut wordt en de interfaces, die er zijn tussen de EUC-omgeving en het centrale informatiesysteem.

Behalve risico's heeft EUC ook voordelen. Gezien de aard en het onderwerp van dit artikel zijn deze voordelen wat minder aan de orde gekomen. Voordelen zijn onder andere:

- EUC ontwikkelt nieuwe vaardigheden bij de gebruikers. De gebruikers leren om zelfstandig en op creatieve wijze hun eigen problemen op te lossen.
- EUC kan een goede voedingsbodem creëren voor innovaties. Vooral in kennisintensieve bedrijfstakken kunnen in EUC getrainde medewerkers innoverende impulsen aan de organisatie geven.
- EUC kan leiden tot meer pluriforme en geavanceerde beslissingsondersteunende informatie en dientengevolge (mogelijk) tot betere beslissingen.
- EUC brengt vooral met betrekking tot de pc lagere kosten met zich mee en heeft daardoor geautomatiseerde gegevensverwerking binnen het bereik van kleinere organisaties gebracht.
- End-users hebben de vrijheid om zelf beslissingen te nemen ten aanzien van het tijdstip en de wijze waarop vervulling van hun informatiewensen plaatsvindt.

Bij het door het management tegemoet treden van het verschijnsel EUC gaat het erom, dat een bewuste afweging wordt gemaakt tussen de risico's, die aan EUC verbonden zijn en de voordelen die EUC aan de organisatie te bieden heeft. Dit impliceert dat EUC als een op zichzelf staande activiteit in de organisatie geïdentificeerd dient te worden en dat EUC de aandacht van het topmanagement verdient. Dit houdt in dat men een EUC-beleid moet voeren.<sup>14</sup> In dit beleid zal tot uiting moeten komen wat EUC betekenen kan en welke concrete doelen men in de komende periode wil bereiken. Daarnaast zal een afweging dienen plaats te vinden welke van de te verwachten risico's men aanvaardbaar acht en welke beperkingen men de end-user in verband daarmee wenst op te leggen. Door op de hiervoor omschreven wijze de interne controleproblematiek rond EUC tegemoet te treden, kan men in een or-

ganisatie een klimaat creëren, waarin EUC enerzijds gedijen kan en anderzijds toch voldoende zekerheden worden ingebouwd, zodat men niet voor onaangename verrassingen komt te staan. Dit klimaat van beheersing is ons inziens althans de beste voedingsbodem waarin EUC tot volle wasdom zal kunnen komen en waarin de organisatie optimaal de vruchten zal kunnen plukken, die EUC te bieden heeft.

## Literatuur

- M. Alavi et al., Strategies for end user computing: An integrative framework, *Journal of information systems*, winter 1987-1988 pp. 28-48.
- G.R. Baker et al., *Computer Control Guidelines*, second edition, The Canadian institute of chartered accountants, 1986.
- M. Beheshtian et al., Strategies for managing user developed systems, *Information and management* 12, 1987 pp. 1-7.
- J.C. Henderson et al., Managing end-user computing for competitive advantage, *Sloan management review*, winter 1986 pp. 3-14.
- E. Huizingh, 10 jaar persoonlijk computergebruik, *Informatie* jaargang 32 nr. 6, 1990 pp. 545-553.
- R.L. Leitheiser et al., Service support levels: An organized approach to end-user computing, *MIS Quarterly*, december 1986 pp. 337-349.
- C.J. Leong, Procedures and controls for micro-based accounting systems, *Journal of accountancy*, january 1988 pp. 111-113.
- P.G. MacLaine Pont, De PC als veilig werkstation, *Bank- en effectenbedrijf*, januari/februari 1988 pp. 5-9.
- J. Medick, Controls in the design of end-user systems, *Edpacs*, february/april 1989 pp. 1-11 en pp. 7-11.
- NEN-ISO 9001: Kwaliteitssystemen, model voor

kwaliteitsborging bij het ontwerpen/ontwikkelen, het vervaardigen, het installeren en de nazorg. NNI 1988.

NEN-ISO 9004: Kwaliteitszorg en de elementen van een kwaliteitssysteem, richtlijnen. NNI 1989.

G.A. Perschke et al., Micro's in accounting, *Journal of accountancy*, april 1986, pp. 107-111.

M.I. Sobol, Local area networks: new concerns for accountants, *Internal auditor*, february 1988 pp. 33-35.

M. Sumner et al., Information systems strategy and end-user application development, *Data Base*, summer 1987 pp. 19-30.

H. Teas, A self-audit of microcomputer controls, *Edpacs*, december 1984 pp. 1-5.

## Noten

- 1 Zie bijvoorbeeld Huizingh over de opkomst van persoonlijk computergebruik.
- 2 Zie Beheshtian.
- 3 Zie onder andere Henderson.
- 4 Zie Huizingh.
- 5 Zie Computer Control Guidelines, in het hoofdstuk over 'distributed computing'.
- 6 Zie Beheshtian.
- 7 Idem.
- 8 Medick heeft ten aanzien van een aantal aspecten een checklist ontworpen.
- 9 Computer Control Guidelines, in het hoofdstuk over 'distributed computing'.
- 10 Zie Sobol.
- 11 Zie MacLaine Pont.
- 12 Zie ook Leitheiser over de rol van de centrale automatiseringsafdeling en Leong over procedures in een pc-omgeving.
- 13 Dit kan gebeuren volgens het NEN-ISO model.
- 14 Zie voor beleidsstrategieën Alavi en Henderson.