Van automatisering en controle tot IT-audit

Prof. A.W. Neisingh RE RA

Hoe het begon

In de jaren zestig en begin zeventig startten organisaties met de introductie van computers ten behoeve van de geautomatiseerde gegevensverwerking. Op dat moment waren de toepassingen veelal administratief van aard en vond deze introductie plaats in situaties waar grote hoeveelheden gegevens moesten worden verwerkt. Organisaties zouden niet verder hebben kunnen groeien indien de processen handmatig hadden moeten plaatsvinden. Wie herinnert zich niet – met name de ouderen onder de lezers – de stop op de uitgifte van gironummers door de toenmalige Post Cheque- en Giro Dienst jaren daarvoor.

De accountant kreeg in die jaren derhalve met het fenomeen automatisering te maken. Het waren omvangrijke processen ten gevolge van de veelheid aan gegevens doch nog alle batchgewijze ingericht. Met andere woorden invoervastlegging stapelsgewijs, waarna de verwerking plaatsvond en nieuwe bestanden werden opgebouwd. De organisatie was in staat dagelijks de volledigheid en juistheid van de geautomatiseerde gegevensverwerking vast te stellen. De accountant werd voor een ander probleem geplaatst en wel: hoe ga ik om met deze massaliteit aan gegevens. De aanpak was eenvoudig. Het gebruik van auditsoftware deed zijn intrede. Enkele softwarehouses leverden standaardauditprogrammatuur, die op bepaalde machinetypes kon worden geïnstalleerd. Door het definiëren van parameters kon de bij de controle betrokken accountant bepalen of er moest worden geteld, vergeleken, steekproeven getrokken en dergelijke. Voor gebruik van deze auditsoftware was het nodig dat de betrokken accountant naar het computercentrum van de cliënt ging om de tape te laden, de besturingskaarten te maken, alsmede vervolgens de selecties definieerde en uiteraard bij de verwerking aanwezig was om na afloop de output en de standaardauditsoftware mee te nemen, alsmede om ervoor te zorgen dat geen kopie van de programmatuur op het systeem van de gecontroleerde achterbleef. Voor de 'normale' accountant betekende dit al snel een stap te ver. En zo ontstond de AC-accountant ofwel de accountant gespecialiseerd op het gebied van automatisering en controle. Deze voorloper van de IT-auditor was thuis in het gebruik van auditsoftware, op het gebied van job control language (de besturingskaarten) alsmede het parametriseren van het standaardauditpakket. En zo is de carrière van menig AC-accountant in de nachtelijke uren gestart bij grote cliënten, want de gewone gegevensverwerking moest eerst worden beëindigd, alvorens de AC-accountant zijn programmatuur kon laden en verwerken. Immers, de computersystemen verwerkten maar één job tegelijk en niet in multiprogrammering, zoals thans het geval is.

Bijzondere problemen manifesteerden zich redelijk snel. Zo was het niet altijd mogelijk de auditsoftware op een bij de cliënt aanwezige computer te installeren en was het derhalve nodig kopieën van bestanden mee te nemen om die op een andere plaats te converteren naar een formaat dat door de auditsoftware kon worden gehanteerd. Op die wijze gebeurde het dan ook dat maandelijks een schijvenpack werd opgehaald bij een cliënt in Cuijk, in Haarlem werd 'vertaald' naar een tape in zeven kanalen, waarna in Amsterdam de conversie van die tape naar een tape met negen kanalen plaatsvond en vervolgens de verwerking op het eigen rekencentrum van toen nog Klynveld Kraaijenhof & Co. Zelfs die dag per maand voor vervoer, conversie en dergelijke was zeer efficiënt in de aanpak van de controle.

In die jaren is uitgebreid gepubliceerd over het gebruik van de computer door de accountant. Vaktechnische vragen waren daarbij uitdrukkelijk aan de orde, zoals waar vindt de verwerking plaats van de auditsoftware in verband met mogelijke beïnvloeding door de gecontroleerde, hoe wordt de programmatuur gedocumenteerd, omdat deze onderdeel uitmaakte van het controleprogramma van de accountant, wie maakt de auditsoftware, moet de verwerking altijd worden bijgewoond, enz. Bovendien ontstonden er technieken die in het kader van de controle op de beheersing van het gebruik van automatisering een rol konden spelen: te denken valt aan integrated test facilities, tracking en tracing, enz.

Op enig moment werd afgestapt van het gebruik van standaardsoftware en werd overgegaan op het tailormade ontwikkelen van controleprogrammatuur ten behoeve van specifieke cliënten. In de jaren zeventig werkten zo circa 20 à 25 programmeurs bij voortduring aan het ontwikkelen, onderhouden en verwerken van controleprogrammatuur. Totdat de PC zijn intrede deed en uit een kritische analyse bleek dat zeker 90% van de toen lopende toepassingen eenvoudig zou kunnen worden overgezet naar de PC. De reden was eigenlijk heel simpel: accountants wilden tellen, vergelijken, steekproeven trekken en dergelijke, zodat standaardsoftware voor gebruik op de PC een zeer doelmatige oplossing leek te zijn. In studieopdrachten uitgevoerd door 'Bikkers' werd aandacht besteed aan mogelijkheden om de PC van de accountant te verbinden met de computer van de cliënt, opdat geautomatiseerd gegevensbestanden konden wor-

den overgehaald en vond onderzoek plaats naar een 'gebruikersvriendelijke accountantsinterface'. Bedieningsgemak voor de accountant stond immers voorop.

In de loop van die jaren raakten accountants ervan overtuigd dat op termijn niet zou kunnen worden volstaan met uitsluitend bestandsonderzoeken, doch dat moest worden overgegaan tot het onderzoeken van geautomatiseerde gegevensverwerkende systemen (de typologie van systemen veranderde van batch via on line naar online/real-time) en van de kwaliteit van de organisatie van het rekencentrum. Niet uit het oog moet worden verloren dat in die jaren computersystemen met een intern geheugen van 32K een volledige bemanning vereisten, alsmede wellicht nog meer ruimte.

Onderzoek van informatiesystemen

Zoals gezegd werd het accountants al snel duidelijk dat inzicht moest worden verkregen in de functionaliteit en de controlemogelijkheden van geautomatiseerde informatiesystemen om de aanpak van de accountantscontrole te kunnen definiëren. Casestudies werden uitgewerkt aan de hand van daadwerkelijke praktijkgevallen en methodieken ontwikkeld. Vanuit het Canadian Institute for Certified Accountants kwamen de computer control guidelines en computer audit guidelines, waarbij de audit guidelines met name waren gericht op de beoordeling van informatiesystemen. Van die systematiek is ons nog bijgebleven dat een papierwinkel in het leven werd geroepen om in ieder geval te kunnen aantonen dat aan dossiervorming de nodige aandacht werd besteed. Niettemin was de methodiek heel systematisch opgebouwd en werd toen al duidelijk dat het noodzakelijk was een zeer gesystematiseerde werkwijze te hebben om uiteindelijk de meest essentiële tekortkomingen, doch ook de goede punten op een adequate wijze te kunnen vastleggen om de controleaanpak te kunnen definiëren respectievelijk in de richting van de management letter punten van aandacht te verzamelen. Ook in Nederland stonden de ontwikkelingen vanzelfsprekend niet stil en zo werd binnen (nog steeds) Klynveld Kraaijenhof & Co de CASA-methode ontwikkeld (Cursus Aanpak Systeembeoordeling en Accountantscontrole), waarna alle aanpakken uit de studie onder de auspiciën van het NIVRA nog eens werden bestudeerd. In de beginfase hadden accountants nog overwegend te maken met batchgewijze georiënteerde informatiesystemen en enige on-linesystemen. Naarmate de jaren verstreken deed uiteindelijk on-line/real-time-gegevensverwerking met databasemanagementsystemen haar intrede en toen werd het dus moeilijk. Er was sprake van het migreren van controlemaatregelen naar hogere softwarelagen, dat wil zeggen oorspronkelijk op papier aanwezige functie- en taakverdeling binnen organisaties werd verankerd in het toegangscontrolesysteem van de computer, alsmede in de wijze waarop de subschema's binnen het databasemanagementsysteem waren gedefinieerd en verankerd. Waar accountants ervan overtuigd waren dat de beoordeling van controle- en beveiligingsmaatregelen in geautomatiseerde systemen primair door hen diende te worden uitgevoerd, bleek al snel dat de technologie zodanig ingewikkeld werd dat wel van een ambitieuze doelstelling sprake was.

De beoordeling van de kwaliteit van de beheersmaatregelen met betrekking tot de geautomatiseerde gegevensverwerking heeft betrekking op het traject van invoervastlegging tot en met uitvoerverstrekking. Een onderscheid dient daarbij te worden gemaakt tussen enerzijds het gedeelte van de verwerking dat binnen de computer plaatsvindt en waar – voor wat betreft internecontrolemaatregelen – wordt gesproken over geprogrammeerde controles en anderzijds de controles in de gebruikersorganisatie. Deze controlemaatregelen tezamen vormen de toepassingscontroles of application controls. Naarmate de tijd voortschrijdt wordt duidelijk dat de kwaliteit van beheersmaatregelen in toepassingsprogrammatuur uiteraard belangrijk is, doch dat in steeds verdergaande mate moet worden gesteund op een kwalitatief goede organisatie van informatie- en communicatietechnologie. Het probleem bij de toepassingen wordt namelijk steeds meer dat ten gevolge van berekeningen, vergelijkingen, inhoudingen en dergelijke in het proces van de geautomatiseerde gegevensverwerking het directe verband tussen invoer, reeds in de systemen aanwezige gegevens en de uitvoer niet op eenvoudige wijze dan wel in het geheel niet kan worden gelegd. De opkomst van electronic data interchange is daarvan een typerend voorbeeld.

Ook internationaal is duidelijk geworden dat moet worden gestreefd naar een universele aanpak van de methode waarop systemen worden onderzocht. En zo is binnen KPMG op enig moment de methode System Review Services ontstaan, die in 1998 heeft plaatsgemaakt voor de Business Process Analysis-aanpak.

Er was en is een voortdurende tendens waarneembaar om cursussen door KPMG EDP Auditors (en voorheen door de AC-accountants) te laten ontwikkelen en de kennis en ervaring over te dragen aan de algemene controlepraktijk. In die jaren (midden jaren zeventig) ontstond dan ook het instituut van AC-parttimer, iemand die een uitgebreide opleiding met name op het terrein van het onderzoek van geautomatiseerde gegevensverwerkende systemen en het beoordelen van automatiseringsorganisaties op hoofdlijnen heeft gehad. Zo werd zelfs een cursus van on-line/real-time-systemen inclusief databases ontwikkeld, waarbij zelfs computeruitdraaien van het databasemanagementsysteem werden gebruikt.

Eveneens in die periode werden accountants geconfronteerd met aspecten van volledigheid van het testen van toepassingsprogrammatuur. De vraag kwam naar voren of uitspraken zouden kunnen worden gedaan met betrekking tot de volledigheid van testgevallen. Daaruit ontstond het tool Cobol Oriented Missed Branch Indicator (COMBI, een vondst van Andries Kamstra). Het principe was erop gebaseerd dat na iedere vraagstelling in de programmatuur een doorlopend nummer werd toegekend aan die tak in de programmatuur. Vervolgens werd na verwerking van de testgevallen een overzicht gegeven van de takken (branches) die niet waren geraakt en waarvoor aanvulling van de testgevallen noodzakelijk zou zijn dan wel zou er sprake zijn van mogelijk frauduleuze takken in de programmatuur.

Beoordeling automatiseringsorganisaties

Al vrij snel werd duidelijk dat ook de kwaliteit van de automatiseringsorganisatie van invloed is op de betrouwbaarheid van de verwerking van geautomatiseerde informatiesystemen. Duidelijk werd dat 'manipulerend' kon worden omgegaan met job control language, waarbij verplichte controlemogelijkheden konden worden overgeslagen. Een reden temeer derhalve om de aandacht te richten op functiescheidingen en procedures zoals die binnen een automatiseringsorganisatie aanwezig dienen te zijn en te zijn verankerd. Zichtbaar werd dat de activiteiten van zogenaamde AC-accountants zich verplaatsten van systeemonderzoeken (zeker de eenvoudige) naar het beoordelen van complexe informatiesystemen tot het beoordelen van de automatiseringsorganisatie op hoofdlijnen. Het onderzoek op hoofdlijnen richtte zich in eerste aanleg op het beoordelen van de functie- en taakverdeling binnen automatisering alsmede ten opzichte van de gebruikersorganisatie, waarover zelfs NIVRA-publicaties het licht zagen (organisatorische plaats van de automatisering in organisaties). Verder werd, zeker in de aanvang, de nadruk gelegd op de beoordeling van de maatregelen van fysieke beveiliging en van de kwaliteit van een calamiteitenopvangplan. Immers, in situaties waarin nog steeds sprake is van een batchgewijze gegevensverwerking, was het opportuun maatregelen te treffen waardoor die gegevensverwerking op eenvoudige wijze kon worden zeker gesteld en dat zijn in eerste aanleg de maatregelen van fysieke beveiliging, met daarachter ter zekerheid een calamiteitenopvangplan. Pas later, toen de ontwikkeling van batchomgevingen naar on-line- en on-line/real-time-omgevingen zich voortzetten, kwam de betekenis naar voren van de kwaliteit van de logische beveiliging, alsmede van de kwaliteit van procedures, richtlijnen en maatregelen in de automatiseringsorganisatie. Te denken valt in dit verband aan de regeling van de toegangscontrole, back-up- en recoverymaatregelen, test-, acceptatie- en overdrachtsprocedures alsmede bibliotheekbeheer en dergelijke. Deze ontwikkeling plaatste de accountant, doch evenzeer de AC-accountant voor een probleem: kennis en ervaring met betrekking tot deze objecten van onderzoek waren uiteraard niet aanwezig, want vereisten een redelijke mate van 'technische' kennis. Het ging immers niet meer om uitsluitend de opzet, doch veel meer om het daadwerkelijk bestaan van de gedefinieerde functie- en taakverdeling, procedures en voorschriften.

Waar de onderzoeken primair waren bedoeld ter ondersteuning van de accountant in zijn rol van controleur van de jaarrekening, werd steeds meer door het management onderkend dat EDP-auditors een toegevoegde waarde leverden. Zij stelden vast of de kwaliteit van de automatiseringsorganisatie daadwerkelijk voldoende was en 'in control', terwijl waardevolle adviezen ter verbetering konden worden gegeven. De accountant ten slotte worstelde nog vele jaren en misschien nu nog wel met de implementatie van de bevindingen van de EDP-auditor aangaande de kwaliteit van de beheersing van de automatiseringsorganisatie op de interne controle en de accountantscontrole. De discussie over steunen op de goede kwaliteit van de automatisering vindt haar basis in de ontwikkeling die zich met betrekking tot IT voordeed en wel een toenemende complexiteit en het gebruik van geautomatiseerde informatieverzorgende systemen waarbij geen directe relatie meer ligt tussen invoer, reeds aanwezige gegevens en de uitvoer uit de verwerking.

PC in de auditpraktijk

Vooruitziende blikken maakten al snel duidelijk dat de accountant ooit met PC's naar cliënten zou gaan. Het werd reeds eerder in dit artikel gemeld. De audittoepassingen die op de computersystemen bij KPMG werkten, waren duur in onderhoud en in voorbereiding, terwijl inmiddels was gebleken dat accountants met standaardtoepassingen een belangrijk deel van hun auditwerkzaamheden konden uitvoeren. Schoorvoetend deed de PC zijn intrede in de auditpraktijk, echter – mede ten gevolge van de dalende prijzen in de PC-markt – nam de PC-dichtheid in de accountantscontrolepraktijk belangrijk toe. Het nodigde aanvankelijk ook niet uit om met een PC door het leven te gaan. De computersystemen waren meer transportable dan portable.

Het gebruik van PC's in de controlepraktijk brengt ons echter niet slechts zegeningen. Het blijft van belang ondanks het gebruik van geautomatiseerde tools met zekere regelmaat afdrukken op papier te maken, die immers deel behoren uit te maken van de controledossiers. Gedacht kan hierbij worden aan met behulp van geautomatiseerde schematechniektools vastgelegde processchema's, die op eenvoudige wijze in volgende jaren zijn te onderhouden. Echter, in verband met de eisen te stellen aan het dossier dient per jaar uiteraard een geactualiseerde beschrijving aanwezig te zijn en zo zal dus ieder jaar een afdruk moeten worden gemaakt (dan wel een kopie van een diskette) en in het dossier moeten worden opgenomen. Hetzelfde kan gelden voor teksten van rapporten en management letters, waarop door leidinggevenden/verantwoordelijken voor de uitvoering van de controleopdracht wijzigingen worden aangebracht. De betrokkenheid van dergelijke functionarissen blijkt dan slechts uit de elektronisch aangebrachte wijzigingen op de tekst. Afdrukken zouden eveneens in het dossier moeten worden bewaard om ieders verantwoordelijkheid later zo nodig te kunnen aantonen. Verder kan een en ander natuurlijk gelden voor mailberichten, die thans op grote schaal worden gebruikt en die vaak belangwekkende mededelingen bevatten met betrekking tot ontwikkelingen bij de gecontroleerde, analyses van posten van de jaarrekening, discussies over punten in de management letter en dergelijke. Papierloos zal een accountantsdossier vooralsnog dus niet zijn.

De portabiliteit van de PC's leidde ook tot minder gewenste ontwikkelingen: diefstal vanaf bureaus, uit auto's, respectievelijk bij inbraken in woonhuizen nam toe. De lopende discussie over het encrypten van de inhoud van de vaste schijven kreeg daardoor een andere wending. Het mocht niet gebeuren dat ten gevolge van verlies van PC's informatie over cliënten en/of over de eigen organisatie op straat terecht zou komen. Nu dat punt is geregeld, is een nieuwe discussie gestart en wel die betrekking heeft secure e-mail; tussen accountant en cliënt worden steeds meer berichten elektronisch uitgewisseld, waarvoor echter een zekere mate van vertrouwelijkheid geldt.

Voor KEA heeft deze ontwikkeling van gebruik van de PC ook nadelige kanten gehad. Een succesvolle ontwikkeling van toepassingen op grote computersystemen was dat de support- en programmingactiviteiten binnen KEA die erop waren gericht de controlepraktijk te ondersteunen, een kweekvijver vormden voor toekomstige EDP-auditors. Zeker in een tijd dat nog geen sprake was van enige uniformering in de opleiding met betrekking tot EDP-auditing en er evenmin postdoctorale opleidingen bestonden, vormde deze support- en programminggroep een waardevol onderdeel van KEA. Ook thans nog zijn medewerkers bij KEA werkzaam die ooit in deze afdeling zijn begonnen.

De dienstverlening verbreed

Duidelijk werd dat de invloed van de kwaliteit van de algemene maatregelen van interne controle en beveiliging op de mogelijkheid tot beheersing van de automatiseringsorganisatie en daarmee van de organisaties als geheel en de invloed op de accountantscontrole van niet te onderschatten betekenis waren. De leiding van KEA besloot de dienstverlening te verbreden door systeemprogrammeurs, bestuurlijke informatiekundigen, ingenieurs informatica en dergelijke aan de organisatie te binden. Tot slot zelfs juristen. Op deze wijze is een breed palet aan dienstverlening ontstaan. De KEA-organisatie heeft ook door haar voorlopersrol binnen de branche model gestaan voor de vorming van andere EDP-auditorganisaties zowel bij interne als externe accountantsdiensten.

Naarmate de integratie van informatie- en communicatietechnologie verder vorm kreeg vond ook een uitbreiding van de kennis en daarmee van de dienstverlening in die richting plaats.

In deze bundel treft u van de hand van KEA-auteurs artikelen aan, waaruit de breedte van het vakgebied waarop EDP-audit thans fungeert, duidelijk wordt.

Opleidingen en onderzoek

Een vooraanstaande praktijk heeft als missie mede een stimulans te geven aan onderzoek op het vakgebied. Het betekent dat enerzijds veel effort is gestoken in het tot stand brengen van opleidingen zowel voor de interne KPMG-accountantsmarkt als ten behoeve van open inschrijving. Verder heeft KEA een belangrijke bijdrage geleverd – en levert deze nog steeds – aan het universitair onderwijs op het gebied van zowel EDP-auditing als waar het gaat om de invloed van het gebruik van informatie- en communicatietechnologie op de beheersing van organisaties en op de accountantscontrole. Het betekende enerzijds het opbouwen van een EDP-auditingopleiding naar verschillende modellen en anderzijds het inrichten van nieuwe leerstoelen op het gebied van accountantscontrole en administratieve organisatie. Vanzelfsprekend hebben zowel betrokkenen als veel medewerkers uit de organisatie veel gepubliceerd, hetgeen onder meer blijkt uit het al sinds 25 jaar verschijnen van het tijdschrift Compact, tijdschrift voor EDP-auditing. Een publicatie die is ontstaan om te voorzien in de behoefte van accountants werkzaam in de algemene controlepraktijk en deze te informeren over ontwikkelingen op het gebied van informatie- en communicatietechnologie en de consequenties die dat voor de accountantscontrole zou hebben. Het tijdschrift Compact, dat sedert een aantal jaren zesmaal per jaar verschijnt, voorziet duidelijk in de behoefte van hen die net in de EDP-auditpraktijk werkzaam zijn dan wel daarin een veeljarige ervaring hebben, en evenzeer in die van accountants werkzaam in de algemene controlepraktijk.

Een organisatie als die van KEA besteedt vanzelfsprekend veel tijd aan het ontwikkelen van nieuwe tools en technieken op het brede terrein van EDP-audit. Waar is begonnen met methoden voor de aanpak van de beoordeling van geautomatiseerde informatiesystemen en het in kaart brengen van de zogenaamde general IT controls (het stelsel van algemene maatregelen van interne controle en beveiliging), zijn belangrijke publicaties verschenen als computeraudit guidance notes in verband met de beoordeling van de daadwerkelijke implementatie van controle- en beveiligingsmaatregelen in besturingssystemen van computers, toegangscontrolesystemen, databasemanagementsystemen en dergelijke. Inmiddels is in breder verband in samenwerking met interne accountantsdiensten gepubliceerd op het gebied van Unix-beveiliging, Internet-beveiliging, inbelbeveiliging en dergelijke. En de ontwikkelingen staan niet stil. Zo is enkele jaren geleden gestart met de ontwikkeling van een praktijk op het gebied van Trusted Third Parties. Dit onderwerp maakt thans deel uit van een inventarisatie naar secure electronic commerce, een ontwikkeling die als strategisch kan worden gekenschetst.