Jaarrekeningcontrole en EDP audit

W.G. van der Poel en J. Waardenburg

1 Inleiding en probleemschets

Het primaire object van onderzoek naar de getrouwheid van de jaarrekening is de te certificeren jaarrekening zelve. Deze is een vastlegging van een feitelijke situatie, waarbij het van belang is vast te stellen hoe deze situatie wordt weergegeven (waarderingsgrondslagen, presentatie en dergelijke) en hoe de feiten tot stand zijn gekomen (betrouwbaarheid informatie). De algemeen accountant die de verklaring bij de jaarrekening afgeeft, is verantwoordelijk voor de verrichte werkzaamheden die leiden tot een deugdelijke grondslag.

Al naar gelang de aard en omvang van de automatisering van de bedrijfs- en financiële processen zal de EDP audit in de huidige controle-aanpak een bepaalde plaats innemen. Daar waar de automatisering in het proces van totstandkoming van de gegevens in de jaarrekening dominant is, zal de EDP audit zelfs een sleutelfunctie vervullen voor de in het kader van de controle te verrichten werkzaamheden. De beoordeling van de administratieve organisatie en interne controle die verband houden met de automatisering is het werkterrein van de EDP auditor en zal van grote invloed kunnen zijn op de verder te verrichten controlewerkzaamheden. Er dient derhalve ook sprake te zijn van een goede samenwerking, een duidelijke communicatie en afstemming tussen de algemene controle en de EDP audit.

In de huidige controle-aanpak vindt een zekere fasering plaats, waarbij EDP audit een duidelijke plaats heeft. In de eerste plaats zal vanuit de algemene controle in samenspraak met de EDP auditor een afweging plaatsvinden waarin de betrokkenheid van EDP audit wordt vastgesteld. Dit is de fase van strategiebepaling. Voorts zal, indien automatisering van essentieel belang is bij de totstandkoming van materiële posten in de jaarrekening, een beoordeling plaatsvinden van de automatiseringsorganisatie en technische infrastructuur. Dit vormt de fundering voor de beoordeling van de informatiesystemen, omdat hierbij onder meer vastgesteld wordt in hoeverre gesteund kan worden op geprogrammeerde controlemaatregelen en hoe en waar de functiescheiding is geregeld. De gegevensgerichte aanvullende controlewerkzaamheden in het kader van de jaarrekeningcontrole worden deels bepaald door de uitkomsten van de EDP audits. Hierbij zal een (gegevensgerichte) toetsing plaatsvinden van de werking van de informatiesystemen. Veelal zullen deze controles met behulp van audit software geschieden en gericht zijn op selectie van uitzonderingssituaties.

In dit artikel wordt in paragraaf 2 een korte algemene uiteenzetting gegeven van de huidige controle-aanpak, met name komen hierbij de verschillende vormen van risico in het kader van de controle aan de orde. Paragraaf 3 behandelt de relatie tussen de EDP audit en de algemene controle.

W.G. van der Poel RA CISA is vennoot van Coopers & Lybrand Dijker Van Dien. Vanaf 1984 is hij werkzaam in de EDP audit en informatiebeveiliging.

J. Waardenburg RA is vennoot van Coopers & Lybrand Dijker Van Dien. Vanaf 1984 is hij werkzaam in de EDP audit en informatiebeveiliging

In paragraaf 4 en 5 wordt een verdere verdieping weergegeven van de EDP audit op de automatiseringsorganisatie en technische infrastructuur, en de beoordeling van informatiesystemen. Hierbij wordt tevens aangegeven welke aanvullende controlemaatregelen door de algemeen accountant moeten worden verricht bij geconstateerde leemten in de administratieve organisatie van de geautomatiseerde gegevensverwerking. Paragraaf 6 geeft een korte behandeling over de ondersteuning van EDP audit bij aanvullende controlewerkzaamheden. Het artikel wordt afgesloten met een samenvatting.

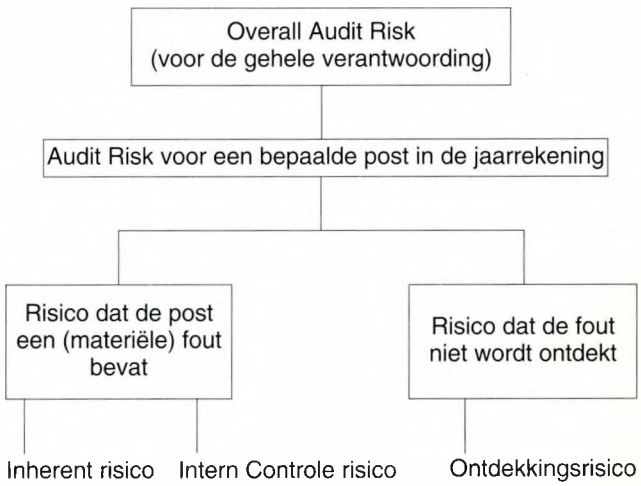
2 Controle-aanpak

In de toonaangevende vakbladen zijn de afgelopen periode met een zekere regelmaat publikaties verschenen over de huidige controle-aanpak. Deze aanpak is gebaseerd op Statements on Auditing Standards (SAS) nr. 47 van het American Institute of Certified Public Accountants (AICPA), getiteld Audit Risk and Materiality in Conducting an Audit: Audit Risk Model.
In SAS nr 47 wordt onderscheid gemaakt tussen de volgende vormen van risico's:

- Overall Audit Risk (controle- of accountantsrisico voor de gehele verantwoording: het risico dat de accountant loopt met betrekking tot een materiële onjuistheid in de jaarrekening);
- Audit Risk (accountantsrisico voor een bepaalde post: het risico dat een bepaalde post materieel onjuist is);
- Inherent Risk (inherent risico: het risico dat voortvloeit uit de omgeving en de branche betreffende post in de jaarrekening);
- Internal Control Risk (intern beheersingsrisico: de risico's ten aanzien van de administratieve organisatie en interne controle, dat ten gevolge van tekortkomingen in de interne beheerstructuur onjuistheden niet opgemerkt worden);
- Detection Risk (ontdekkingsrisico, het risico dat onjuistheden niet ontdekt worden bij de controlewerkzaamheden, waaronder cijferbeoordeling en steekproeven).

Schematisch is dit als volgt weer te geven (zie schema 1):

Schema 1



Het is uiteraard zo dat er sprake is van een zekere relatie tussen de verschillende vormen van risico's. De inherente risico's hebben een grote invloed op de opzet en werking van de administratieve organisatie en interne controle. Het oordeel over de administratieve organisatie, automatisering en interne controle zal dan ook mede gebaseerd zijn op de inherente risico's. Dit impliceert dat er sprake is van een zekere normering met betrekking tot de administratieve organisatie, en dus ook de EDP audit. Dit zijn uiteraard geen algemeen aanvaarde normen, maar normen die gebaseerd zijn op de specifieke omgeving en situatie van het controle-object, en grotendeels gebaseerd op empirische grondslagen en professional judgement. In het vervolg van het controletraject zijn eventuele leemten in de administratieve organisatie en interne controle op zichzelf weer aanleiding tot verdere gedetailleerde controlewerkzaamheden.

Deze controle-aanpak voor de jaarrekeningcontrole geeft een goede positionering van de EDP audit, maar is op zichzelf ook toepasbaar voor de EDP audit. De fasering is immers vergelijkbaar. Zo is bijvoorbeeld de aard van de apparatuurlijn, bijvoorbeeld mainframe, mini of een koppeling van

pc's, een vorm van inherent risico. Eenzelfde geldt voor programmatuur, een MVS operating system zonder toegangsbeveiligingsprogrammatuur schept grote risico's ten aanzien van de functiescheiding. De toegangsbeveiligingsprogrammatuur vormt de interne beheersmaatregel, alsmede de wijze van de implementatie en parameterzetting van deze programmatuur. Bij de beoordeling van de implementatie, parameterzetting en werkwijze met het systeem wordt inzicht verkregen in de interne controlerisico's voor de EDP auditor. Dit geeft weer aanleiding om aanvullende controlewerkzaamheden te verrichten. Dit kan betrekking hebben op de feitelijke autorisaties in het systeem. Hiermee loopt het traject van EDP audit langs dezelfde weg als de algemene controle.

Het is naar onze mening niet zo dat de op risicoanalyse gebaseerde en gestructureerde, controle-aanpak onvoldoende ruimte laat voor de specifieke situatie bij een cliënt en te veel gericht is op het afwerken van vragenlijsten en te weinig rekening kan worden gehouden met het professional judgement, creativiteit en individuele invulling. Met name de inherente risico's die afhankelijk zijn van de branche en cliënt-specifieke aangelegenheden, vereisen een goede kennis en een goed inzicht in de specifieke cliëntsituatie. Door structurering en vastlegging van de risico's wordt juist het professionele judgement inzichtelijk gemaakt. Dit geldt eveneens voor het interne controlerisico.

3 EDP audit in het kader van de jaarrekeningcontrole

De algemeen accountant heeft een aantal doelstellingen bij zijn controlewerkzaamheden. Deze doelstellingen (audit objectives) zijn :

- volledigheid (completeness);
- juistheid en accuratesse (accuracy);
- bestaan (existence);
- waardering (valuation);
- eigendom (rights and obligations);
- presentatie (presentation and disclosure) en eventueel
- toerekening aan verslagperiode (cut off).

Wil de accountant deze doelstellingen realiseren dan is integratie van de EDP audit in de controle van de jaarrekening noodzakelijk ter ondersteuning van de oordeelsvorming. De sterke integratie van automatisering in bedrijfs- en financiële processen veroorzaakt immers een sterke geautomatiseerde administratieve organisatie, waar de basis voor betrouwbare informatievoorziening wordt gelegd. De beoordeling van de met de automatisering verband houdende administratieve organisatie en het bepalen van de interne controlerisico's is het werkterrein van de EDP auditor. De geautomatiseerde informatievoorziening en administratieve organisatie is een zeer belangrijk aandachtspunt bij de beoordeling van de interne controlerisico's.

Indien de EDP auditor bij het controleproces van de jaarrekening betrokken is ontstaat de vraag, wie (algemeen accountant of EDP auditor) nu verantwoordelijk is en voor welke onderdelen. Aangezien de algemene accountant de verklaring bij de jaarrekening afgeeft en ondertekent zal de eindverantwoordelijkheid dan ook onomstotelijk bij hem liggen. Hij zal echter hiervoor moeten steunen op de werkzaamheden en het oordeel van de EDP auditor.
Bij het bepalen van de strategie van de controle zal de EDP auditor een belangrijke inbreng hebben. Indien bij de risico-analyse (zowel inherent risico als mogelijk interne controlerisico) blijkt dat EDP audit-werkzaamheden noodzakelijk zijn voor de oordeelsvorming omtrent de getrouwheid van de jaarrekening zullen goede werkafspraken gemaakt dienen te worden op welke wijze verantwoordelijkheid wordt genomen en kan worden gedragen.
De aard en omvang hiervan is mede afhankelijk van het feit of de EDP auditor deel uitmaakt van dezelfde accountantsorganisatie als de algemene accountant. Indien dit het geval is zal controleaanpak, normering en standaarden, dossierindeling en dergelijke goed op elkaar aansluiten.

De algemeen accountant zal in het geval van geautomatiseerde gegevensverwerking nagaan welke relevante (materiële) posten in de jaarrekening tot stand komen door middel van geautomatiseerde informatiesystemen, en welke posten in de jaarrekening anderszins verband houden met automatisering. Een eerste beoordeling op interne controlerisico's zal dan dienen plaats te vinden.

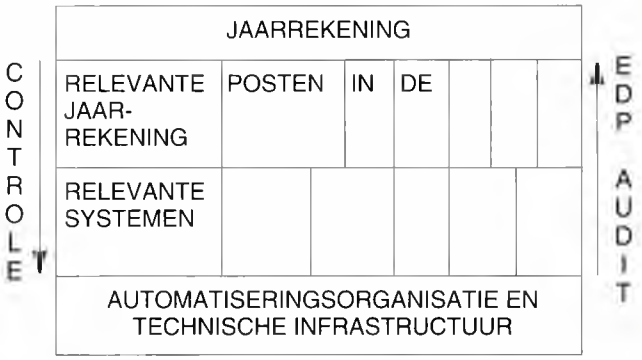
Het valt buiten het bestek van dit artikel om de vraag te behandelen of de eerste beoordeling door de algemeen accountant moet geschieden of door de EDP auditor, dan wel gezamenlijk. De eerste beoordeling draagt een voorlopig en inventariserend karakter. De EDP auditor kan ook achteraf kennis nemen van de kwaliteit van deze voorlopige beoordeling en zijn bevindingen terugkoppelen naar de algemeen accountant.

Aan de hand van de conclusie van deze beoordeling worden verdere EDP audit-werkzaamheden verricht. De algemeen accountant zal in het dossier in ieder geval moeten vastleggen welke punten bij de voorlopige beoordeling aan de orde zijn geweest en welk vervolgtraject is gepland.

Bij de aanvang van (verdere) EDP audit-werkzaamheden zal gestart worden met een onderzoek naar de automatiseringsorganisatie en technische infrastructuur (beoordeling van de general controls of information technology controls). De uitkomst van dit onderzoek geeft weer in hoeverre op de controlemaatregelen in de informatiesystemen kan worden gesteund bij de controlewerkzaamheden.

Schematisch is de benadering van de jaarrekeningcontrole en de EDP audit als volgt weer te geven (zie schema 2):

Schema 2



Uit schema 2 blijkt dat de controle 'top down' uitgaande van de jaarrekening wordt nagegaan, welke objecten en aspecten beoordeeld moeten worden. Indien vanuit de eerste beoordeling en het bepalen van de audit-strategie is komen vast te staan dat EDP audit-activiteiten moeten plaatsvinden zal de EDP auditor daarentegen echter 'bottom up' vanuit de automatiseringsorganisatie en technische infrastructuur te werk gaan.

4 Automatiseringsorganisatie en technische infrastructuur

In het kader van de jaarrekeningcontrole is zoals reeds aangegeven de integriteit van de gegevens van belang. Dit impliceert dat de opslag, de verwerking, de toegang en het transport van gegevens met name relevant zijn.
Bij de beoordeling van de automatiseringsorganisatie en technische infrastructuur komen derhalve over het algemeen de volgende aspecten aan de orde:

- functies, taken en verantwoordelijkheden binnen de automatiseringsorganisatie en van automatiseringsorganisatie naar buiten, de gebruikersorganisatie (de toegang tot de gegevens);
- integriteit van programmatuur, omvattende zowel de integriteit van systeem- als applicatieprogrammatuur, de implementatie en onderhoudsprocedures en het beheer van de wijzigingen (toegang en verwerking);
- toegangscontroles, zowel in logische als fysieke zin (toegang tot de gegevens);

- computerverwerking, bestaande uit de procedures inzake scheduling, job set-up en uitvoering, gebruik van juiste gegevensbestanden, het bewaken en loggen van activiteiten en back-up en recovery (opslag van en toegang tot de gegevens);
- datacommunicatie, waarborgen voor integriteit en vertrouwelijkheid van het gegevensverkeer (transport van de gegevens).

In het kader van de jaarrekening zijn de maatregelen die de continue verwerking van gegevens moeten waarborgen, over het algemeen niet specifiek object van onderzoek hetgeen overigens niet wil zeggen dat de algemeen accountant c.q. de EDP auditor hier geen aandacht aan zal schenken.

Indien geconstateerd wordt dat er zwakke plekken zijn in de automatiseringsorganisatie en technische infrastructuur, is dit van wezenlijke invloed op de verdere controle. Tevens is bij de eerste beoordeling vastgesteld waar de controlemaatregelen zich bevinden, met name is de vraag beantwoord of de maatregelen getroffen zijn in de systeem- of applicatieprogrammatuur. Dit laatste is in hoge mate bepalend voor de verdere controle-acties.

Ter illustratie volgt hier een schema van veel voorkomende zwakheden in de automatiseringsorganisatie en technische infrastructuur en de mogelijke volgende controle-acties, en de mogelijke aandachtspunten voor een management letter (zie schema 3).

Schema 3

Tekortkoming	Acties	Management letter
Onvoldoende omvang en functiescheiding automatiseringsorganisatie	Heroriëntatie controle-aanpak. Extra controle geldstromen en andere belangrijke activa e.d.	Verbetering functiescheiding Frauderisico
Onvoldoende scheiding tussen ontwikkel-, test- en produktie-bibliotheken, geen adequaat programmabeheer	Niet zonder meer kunnen steunen op de geprogrammeerde controles; Geen 'systeemgerichte' controle, c.q. een aangepaste controle	Verbetering programmabeheer Risico's ten aanzien van opzettelijke en onopzettelijke fouten
Onvoldoende beveiliging gegevens, logische toegangsbeveiliging	Mogelijk onvoldoende functiescheiding, heroverwegen controle-aanpak	Beveiligingsmaatregelen i.v.m. waarborgen voor integriteit en vertrouwelijkheid gegevens
Onvoldoende beveiliging bij het aanmaken en verzenden van geautomatiseerd betaalverkeer	Controle achteraf op de uitgaande geldstroom	Preventieve beveiligingsmaatregelen in verband met frauderisico
Systeemprogrammering heeft verstrekkende bevoegdheden	Controle achteraf op kritische processen die mogelijk beïnvloed kunnen worden	Bevoegdheden beperken tot datgene wat noodzakelijk is voor de functie-uitoefening
Utilities met wijzigingsmogelijkheden zijn aanwezig	Extra controle op kritische processen zoals uitgaande geldstromen	Beperking gebruik en interne controle op gebruik
(Zelf gemaakte) exits aan de systeemprogrammatuur aanwezig	Beoordelen change management systeemprogrammatuur en documentatie	Exits beperken, alleen indien strikt noodzakelijk
Onvoldoende integriteitscontroles op bestanden	Beoordelen applicatie c.q. gegevens	Verbeteren controles automatiseringsorganisatie
Onvoldoende administratieve organisatie rondom parameterzetting en tabelinhoud schedulingspakket	Periodiek beoordelen inhoud parameters en tabellen	Verbeteren organisatie en beheer omtrent parameters en tabellen

Vanuit de praktijk is waar te nemen, dat met name het programmabeheer en de logische toegangsbeveiliging in complexe netwerkomgevingen vaak zwakke plekken in de administratieve organisatie zijn.
Dit kan tot gevolg hebben dat er geen adequate functiescheiding aanwezig is met alle risico's die hieraan verbonden kunnen zijn. Ook kan voor de accountant een grote mate van onzekerheid ontstaan omtrent het aanwezig zijn van de geprogrammeerde controles, waar hij bij een 'systeemgerichte' controle juist gebruik van wil maken. Het ontbreken van een audit trail en het steeds verder integreren van processen door geautomatiseerde gegevensverwerking zal het onmogelijk maken om buiten de computer heen te gaan controleren. De uitkomsten van de beoordeling van de automatiseringsorganisatie is dus bepalend voor de verdere controle-aanpak. Ernstige tekortkomingen kunnen zelfs leiden tot onvervangbare interne controle. Veelal laat de praktijk zien dat geconcludeerd moet worden dat geen volledige 'systeemgerichte' controle mogelijk is en dat meer 'gegevensgericht' te werk zal moeten worden gegaan. De EDP auditor vervult in dergelijke situaties een belangrijke rol in het verdere audit-proces.

5 De beoordeling van informatiesystemen

5.1 Algemeen

De accountant is in het kader van de jaarrekeningcontrole met name geïnteresseerd in de betrouwbaarheid van de gegevens die van (materieel) belang zijn in de jaarrekening. Bij de beoordeling van de automatiseringsorganisatie en de technische infrastructuur is vastgesteld of het mogelijk is voor de controle te steunen op de beheersmaatregelen (de administratieve organisatie en interne controle) en of er 'echt systeemgericht' kan worden gecontroleerd.

Het ligt voor de hand de informatiesystemen 'systeemgericht' te beoordelen, waarbij de opzet en werking van processen en de geprogrammeerde controles moet worden vastgesteld.

In de voorgaande paragraaf is aangegeven dat veelal niet zonder meer op de automatiseringsorganisatie en technische infrastructuur kan worden gesteund, hetgeen ook van invloed is op de verdere controle-acties.
Hierbij moet echter worden opgemerkt, dat er sprake is van een aantal 'gegevensgerichte' elementen.

5.2 Werking geprogrammeerde controles

Indien bij de controle geen gebruik gemaakt kan worden van de automatiseringsorganisatie en de technische infrastructuur kan er derhalve onzekerheid ontstaan omtrent de werking van geprogrammeerde controles, de werking van de toegangsbeveiliging en eigenlijk de gehele juiste werking van het systeem. De geprogrammeerde controles zullen dan op bestaan en werking moeten worden getoetst aan de hand van de uitvoer (gegevens).

Al naar gelang de betrouwbaarheid en het belang van de controles zal dit met een meer of minder grote frequente moeten plaatsvinden. Hetzelfde geldt dan voor autorisatietabellen en andere relevante functionaliteiten van het systeem. Beoordeeld moet worden of de onzekerheid in de controle kan worden weggenomen door extra waarnemingen. Zo niet, dan blijft er onzekerheid bestaan omtrent de feitelijke juistheid van de weergave van situaties en gebeurtenissen

Voor het toetsen van de werking van processen en geprogrammeerde controles zal altijd naar de gegevens, de uitkomsten, moeten worden gekeken. Op grond van de bevindingen van de EDP auditor zal de accountant richting geven aan zijn verdere werkzaamheden.

5.3 Opslag gegevens

Gegevens zijn opgeslagen in informatiesystemen en worden gemuteerd door transacties. Bij de beoordeling dient derhalve aandacht te worden geschonken aan de opslag van die gegevens, het integer zijn en het integer houden van de gegevensverzameling. Met betrekking tot de

transacties gaat het met name om die transacties die kritische gegevens kunnen muteren. Het is van belang de gegevensstructuur van de te beoordelen informatiesystemen vast te leggen teneinde vast te stellen welke gegevens er zijn en vervolgens te bepalen welke gegevens kritisch zijn. Dit heeft nog een ander doel. Voor het in een later stadium van de controle selecteren van gegevens met behulp van audit software moet de gegevensstructuur bekend zijn.

De vast te leggen gegevensstructuur kan, al naar gelang de feitelijke situatie van het te onderzoeken systeem, de logische of fysieke structuur zijn. Bij het gebruik van een database-managementsysteem zal de data dictionary veelal deze informatie direct verschaffen, waarbij echter opgemerkt dient te worden dat ook dan vastgesteld moet worden of deze documentatie betrouwbaar is, omdat niet iedere dictionary een geïntegreerd onderdeel is van het database-managementsysteem.
Bij niet database toepassingen zal deze informatie de fysieke record indeling betreffen.
Door de gegevensstructuur in totaliteit per informatiesysteem vast te leggen en de onderlinge relatie en afhankelijkheid weer te geven is snel te bepalen welke gegevens uit oogpunt van betrouwbaarheid kritisch zijn. Coderings- of sleutelgegevens die ogenschijnlijk onbelangrijk lijken, kunnen kritisch zijn uit oogpunt van toegankelijkheid en controleerbaarheid van het informatiesysteem. Aan de hand van deze vastlegging kan de algemeen accountant, eventueel in overleg met de EDP auditor gegevens selecteren, matchen en dergelijke met behulp van audit software. De integriteit van de (selectie of extractie van de) gegevensverzameling kan worden vastgesteld door controletotalen en tellingen.

5.4 Integriteit gegevensverzameling

Voorts dient vastgesteld te worden op welke wijze de integriteit van de gegevensverzameling wordt beheerd. Dit kan hebben plaatsgevonden bij de beoordeling van de technische infrastructuur (bijvoorbeeld een samenstel van computerverwerkingsprocedures, zoals cataloguing, scheduling, generatie-validatie en dergelijke, en maatregelen in het database-managementsysteem of een ander hulpmiddel voor file access). Er kan ook sprake zijn van applicatief gebonden controlemaatregelen (bijvoorbeeld controletotalen), geprogrammeerde controles of een samenstel van controlemaatregelen. De controle van de automatiseringsomgeving en technische infrastructuur is derhalve mede bepalend voor de vraag welke systemen beoordeeld dienen te worden.

Indien de integriteit van de gegevensverzameling niet of onvoldoende gewaarborgd is, schept dit een grote mate van onzekerheid ten aanzien van de oordeelsvorming van de algemeen accountant. Slechts in uitzonderingssituaties zal de accountant door middel van aanvullende maatregelen, bijvoorbeeld met behulp van audit software doortellen of matching van bestanden zekerheid kunnen krijgen omtrent de integriteit van de gegevensverzameling.

De integriteit van de gegevens kan mede vastgesteld worden op basis van informatie van functionarissen met tegengestelde belangen. De doelstelling is de rechtmatigheid van de transacties vast te stellen, in de buitenlandse literatuur vaak aangeduid als authorization of transactions, in de Nederlandse vakpers onder de noemer functiescheiding gebracht.

Functiescheiding wordt als een der belangrijke steunpunten gezien voor de betrouwbaarheid van de informatievoorziening. Het ontbreken van of het onvoldoende zijn van functiescheiding kan een objectieve verhindering zijn om een oordeel uit te spreken over de getrouwheid van een verantwoording als geheel. Er is in dat geval sprake van onzekerheden in de controle. De feitelijke juistheid kan niet worden vastgesteld. Slechts in uitzonderingsgevallen kan er sprake zijn van vervangbare (interne) controlemaatregelen. Cijferbeoordelingen, verbandscontroles en inlichtingen van derden kunnen in bepaalde gevallen enige zekerheid geven dat onvoldoende functiescheiding niet heeft geleid tot onbetrouwbare informatievoorziening.

5.5 Functiescheidingen en autorisatie

Het vaststellen van het belang en de beoordeling van de functiescheiding en autorisatie in geautomatiseerde omgevingen is primair het werkterrein van de algemeen accountant. In de sterk geautomatiseerde omgeving zal de EDP auditor opzet, bestaan en werking van de functiescheiding gaan beoordelen. De EDP auditor zal eerst vaststellen waar de relevante functiescheidingen zijn geregeld. Dit kan in de systeemprogrammatuur zijn èn/of in de applicatieprogrammatuur. Indien een en ander in de applicatieprogrammatuur is geregeld moet worden vastgesteld dat deze programmatuur ook daadwerkelijk werkt.
De werkzaamheden van de EDP auditor zijn voorts gericht op de wijze waarop de gebruikers de gegevens benaderen. Gebruikers zullen zich op een bepaalde manier moeten identificeren en er zal een systeem moeten zijn dat vaststelt of de identificatie juist is (authenticiteit). Het zal duidelijk zijn dat voor een adequate functiescheiding het noodzakelijk is dat gebruikers-identificaties persoonsgebonden zijn en de authenticiteit op een deugdelijke wijze door het systeem wordt vastgesteld. Het meest gangbaar is nog steeds het password mechanisme, waarbij de EDP auditor zal beoordelen of dit voldoende waarborgen biedt voor een adequate functiescheiding (vertrouwelijkheid password bestand, periodiek wijzigen password, minimum password lengte en dergelijke). Opzet, bestaan en werking zijn aldus door de EDP auditor vastgesteld. De interne controlerisico's voor de algemeen accountant worden vervolgens aangegeven. Op grond van deze bevindingen zal de accountant aanvullende controlewerkzaamheden verrichten om zekerheid te verkrijgen omtrent de betrouwbaarheid van gegevens, zoals bijvoorbeeld gegevens van derden. Tevens is dit een aandachtspunt voor de management letter.

5.6 Overige werkzaamheden

De EDP auditor kan voorbereidende werkzaamheden verrichten met betrekking tot het gebruik maken van geautomatiseerde hulpmiddelen bij de jaarrekeningcontrole. Bij een grote hoeveelheid gegevens en transacties is het praktisch de autorisatietabellen over te halen naar een eigen geautomatiseerde omgeving van de accountant/EDP auditor. Hierdoor is het relatief eenvoudig door middel van cross references de controle op de functiescheiding uit te voeren, waardoor de accountant zekerheid omtrent de werking van de functiescheiding verkrijgt.

6 EDP audit en aanvullende controlewerkzaamheden

Is er nog een rol van betekenis weggelegd voor de EDP auditor bij de vervolgwerkzaamheden? Cijferbeoordeling is een specifiek controlemiddel dat de algemeen accountant hanteert. Ook de verdere controlewerkzaamheden, zoals het selecteren van posten door middel van steekproeven heeft vaak geen andere relatie met EDP audit dan het gebruik maken van audit software. Dit laatste wordt door verdergaande automatisering van de accountantscontrole en met name de introductie van micro computers en file interrogation programma's vaak door de algemeen accountant verricht. Toch kan door een vergaande integratie tussen de algemene controle en de EDP audit met name de werking van de informatiesystemen verder aandacht krijgen. Door het selecteren van gegevens met behulp van audit software kunnen juist uitzonderingssituaties worden gecontroleerd. Een dergelijke 'audit by exception' maakt het mogelijk naast het verkrijgen van zekerheid over de gegevens de werking van het informatiesysteem in 'extreme' omstandigheden te beoordelen, en te toetsen of foutafhandeling en -procedures correct werken. Selectie van cijfers op grond van voornoemd traject verhoogt de efficiency en waarde van de controle.

7 Samenvatting

In sterk geautomatiseerde omgevingen is EDP audit een geïntegreerd onderdeel van de controle van de jaarrekening. Teneinde dit te effectueren dient er sprake te zijn van een concrete samenwerking tussen de algemeen accountant en de

EDP auditor. De rol van de EDP auditor ligt met name bij het aangeven van interne controlerisico's die verband houden met de automatisering en het bepalen van de daaruit voortvloeiende aanvullende controlewerkzaamheden.

De algemeen accountant is en blijft verantwoordelijk voor de totale werkzaamheden die in het kader van de jaarrekeningcontrole moeten worden verricht. Dit komt mede tot uiting in het ondertekenen van de accountantsverklaring.

De beoordeling van de automatiseringsorganisatie en technische infrastructuur en de beoordeling van informatiesystemen zijn geen los staande zaken.
In het kader van EDP audit-werkzaamheden voor de jaarrekening zal afhankelijk van de audit-strategie en de relatie tussen materiële posten van de jaarrekening, informatiesystemen en automatiseringsopzet, bestaan en werking moeten worden beoordeeld.

De beoordeling van de automatiseringsorganisatie en technische infrastructuur is de fundering voor de EDP audit-werkzaamheden. Een interne controlerisico in dit gebied bepaalt in hoge mate de verdere beoordeling van de informatiesystemen en de aanvullende controlewerkzaamheden. Er kan geen sprake zijn van een marginale toetsing, indien voor de jaarrekening belangrijke informatie met behulp van automatisering tot stand komt.

In het kader van de controle op de jaarrekening is het van belang dat ruime aandacht wordt besteed aan 'gegevensgerichte' elementen. Dit vindt plaats door het vastleggen van de gegevensstructuur, het beoordelen van procedures ten aanzien van kritische gegevens en door de werking van informatiesystemen vast te stellen door middel van deelwaarnemingen.
Door verdere integratie van EDP audit in het controleproces van de jaarrekening zal door het selecteren (met behulp van audit software) van uitzonderingssituaties een grotere zekerheid en beter inzicht worden verkregen in de werking van de administratieve organisatie en de getrouwheid van de jaarrekening.

Literatuur

AICPA, SAS 47.

Blokdijk, J.H., Informatiegerichte analytische controle,*MAB,* november/december 1985.

NIVRA, Meningsuiting 5, 1983.

NIVRA geschrift 53.

Murphy, Michael A. & Xenia Ley Parker, *Handbook of EDP Auditing*, Warren, Gorham & Lamont, 1989.

Murphy, Michael A, Albert H. Decker & Xenia Ley Parker, *Handbook of EDP auditing 1991/1992 Cumulative Supplement,* Warren, Gorham & Lamont 1991.

Leenaars, J.J.A., Functiescheiding in hoog geautomatiseerde omgevingen, *MAB*, maart 1990 .

Poel, W.G. van der, *Logische toegangsbeveiliging. Doelmatige bedrijfsvoering,* maart 1990.

Poel, W.G. van der, *Functiescheiding en beveiliging*, lezing VERA conferentie, december 1991.

Weber, Ron, *EDP Auditing, Conceptual Foundations and Practice,* McGraw Hill, 1989.

Zutphen, L.C. van, EDP Audit; een poging tot verduidelijking, *MAB,* november/december 1985.