EDP-auditor en jaarrekening-controle van vergaand geautomatiseerde organisaties

W. de Korte RE RA

Bij de controle van de jaarrekening van organisaties die in hoge mate zijn geautomatiseerd, zal de accountant bij zijn oordeelsvorming bijzonder afhankelijk zijn van de toepassing van IT bij de gecontroleerde organisatie. De controlemiddelen en -technieken van de accountant zullen bij deze organisaties veelal tekortschieten voor een deugdelijke grondslag. Kan de EDP-auditor vanuit zijn deskundigheid een uitspraak doen over posten in de saldibalans en derhalve de beperkingen van de controlemiddelen en technieken van de accountant compenseren?

Inleiding

Reeds decennia lang neemt de automatiseringsgraad binnen organisaties toe. Taken worden meer en meer geautomatiseerd uitgevoerd. Vele controletaken van gebruikers worden in de vorm van controleprocedures in de toepassingsprogrammatuur opgenomen. Dit heeft mede tot gevolg dat veel controles in de bedrijfsprocessen niet (altijd) meer zichtbaar zijn voor de gebruiker.

Een belangrijk controlemiddel voor de accountant is de beoordeling van de opzet van de stelsels van maatregelen van interne controle en het vaststellen van de juiste werking daarvan. Het vervallen van zichtbare gebruikerscontroles en functiescheiding noodzaakt de controlerend accountant er steeds meer toe bij de controle van de jaarrekening gebruik te maken van de controles die binnen de automatisering zijn aangebracht. De EDP-auditor zal vanuit zijn deskundigheid de accountant kunnen ondersteunen bij het routinematige deel van de uitvoering van de controle van de jaarrekening.
Veelal krijgt de beoordeling van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking nog weinig aandacht of staat dit los van de jaarrekeningcontrole. In feite blijkt in de praktijk nog steeds een voorkeur te bestaan voor de eertijds gebruikelijke 'audit around the computer'. De EDP-audits worden veelal uitgevoerd ten behoeve van het management en zijn met name gericht op verbeteringen, hetgeen zijn neerslag vindt in de adviesbrief en omdat BW boek II artikel 393 lid 4 dat in een aantal gevallen vereist.
De vraag of de EDP-auditor zich een oordeel moet vormen over de hierboven genoemde (deel)aspecten van de geautomatiseerde gegevensverwerking ten behoeve van ondersteuning van de accountant bij zijn controlerende taken is nu en zeker in de toekomst niet de enig relevante. Momenteel is een aantal organisaties reeds op een zodanige wijze geautomatiseerd, dat controle met behulp van brondocumenten onmogelijk is geworden of op korte termijn onmogelijk zal worden. De accountant zal bij zijn onderzoek naar de getrouwheid van de jaarrekening zonder de geautomatiseerde gegevensverwerking daarbij te betrekken in deze gevallen niet tot een oordeel kunnen komen omtrent de volledigheid, het bestaan en de accuratesse (juistheid) van posten in de jaarrekening.

Dit artikel gaat in op de vraag of het voor een EDP-auditor mogelijk is een uitspraak te doen over beweringen (van posten) in de saldibalans in het kader van de controle van de jaarrekening van organisaties die in hoge mate zijn geautomatiseerd (op basis waarvan de accountant zich vervolgens zelfstandig een oordeel kan vormen).
Het onderwerp leent zich ongetwijfeld voor verdere discussie tussen accountants en EDP-auditors. Dit artikel is een weergave van de aanpak en noodzakelijke werkzaamheden van de EDP-auditor voor het verkrijgen van een deugdelijke grondslag voor het doen van een uitspraak over beweringen (aangaande posten) in de saldibalans in het kader van de controle van de jaarrekening.

Casus Security First Network Bank

De actualiteit van de in de inleiding geschetste vraagstelling wordt ter illustratie verduidelijkt door onderstaande casus.

Security First Network Bank (verder te noemen SFNB) maakt gebruik van de mogelijkheden die door Internet worden geboden. Alle transacties worden door cliënten via Internet en het netwerk van de betaal- en geldautomaten aangeleverd. Het inlezen van de transacties in de geautomatiseerde informatiesystemen (verder te noemen GIS) geschiedt volledig automatisch gepaard gaande met geprogrammeerde invoercontroles. Vervolgens worden de transacties, omgeven door geprogrammeerde controles, automatisch verwerkt in de GIS. Na verwerking worden de mutaties op de rekeningoverzichten van de cliënten automatisch bijgewerkt. Tevens vindt renteberekening en tarifering van transacties (waaronder effecten) periodiek volledig automatisch plaats. De cliënt kan via Internet zijn rekeningoverzichten opvragen. Nagenoeg alle handmatige activiteiten zijn overgenomen door de applicaties of worden uitgevoerd door de cliënt (invoer van transacties). Slechts enkele (controle)werkzaamheden worden door de medewerkers van de bank verricht, waaronder beoordeling van de kredietaanvragen van cliënten. De accountant wordt verzocht de jaarrekening van een verklaring te voorzien. Er zijn bij SFNB nagenoeg geen fysieke brondocumenten voorhanden op basis waarvan de accountant een controle op de volledige en juiste verwerking van transacties (met name ten

behoeve van de verantwoording van de omzetprovisie, transactiekosten vreemde valuta, rentebaten en -lasten en opbrengsten van effectentransacties, herwaardering positie in vreemde valuta en effecten inclusief off-balance-posities) kan verrichten 'om de GIS heen'.

De accountant zal de volledigheid van de registratie van de invoer van geaccepteerde en uitgevoerde transacties moeten kunnen vaststellen. Hiertoe is geen soll-positie vanuit fysieke brondocumenten aanwezig. De geprogrammeerde invoercontroles (onvervangbare maatregelen van interne controle vanwege het ontbreken van een goederenbeweging) dienen zorg te dragen voor volledige, juiste en tijdige registratie (kortom betrouwbaar) van geaccepteerde en uitgevoerde transacties. De accountant zal een systeemgerichte controleaanpak dienen te selecteren als gevolg van het ontbreken van andere controlemiddelen, waarbij gebruik wordt gemaakt van maatregelen van interne controle binnen de automatiseringsorganisatie (general ICT controls) en de applicaties.

Samenwerking accountant en EDP-auditor in geval van complexe GIS

De accountant dient te overwegen in welke mate de GIS van invloed zijn op de controle. De accountant moet voldoende kennis bezitten omtrent de GIS om de (te) verrichte(n) werkzaamheden te kunnen plannen, sturen, begeleiden en beoordelen. Hij dient derhalve te overwegen of er ten behoeve van de controle behoefte is aan specialistische kennis op het gebied van GIS. Indien een deskundige op het gebied van GIS wordt ingeschakeld, dient de accountant de zekerheid te verkrijgen, dat dergelijke werkzaamheden toereikend zijn voor zijn controledoelstellingen, met inachtneming van hetgeen hierover is opgenomen in de Richtlijnen voor de Accountantscontrole. Volgens de Richtlijnen voor de Accountantscontrole blijft de accountant eindverantwoordelijke voor de af te geven accountantsverklaring bij de jaarrekening. De accountant dient zich zelfstandig een oordeel te kunnen vormen omtrent de uitkomsten van de uitvoering van de EDP-audit.

Vanwege het ontbreken van een definitieve richtlijn waarin de samenwerking tussen accountants en EDP-auditors wordt beschreven (de ontwerprichtlijn over de samenwerking is niet aangenomen), wordt bij de beantwoording van de vraagstelling gebruikgemaakt van Richtlijn 621 (Samenwerking Accountant en Actuaris). Het is overigens ook mogelijk dat EDP-auditors binnen de accountantsorganisaties gehouden zijn aan interne kantoorrichtlijnen.

In Richtlijn 621 wordt gesteld dat de actuaris verantwoordelijk is voor de materiële juistheid en toereikendheid van de voorziening voor verzekeringsverplichtingen/pensioenverplichtingen. Naar analogie hiervan kan gesteld worden dat de EDP-auditor verantwoordelijk is voor het deel van de controle, dat door hem wordt uitgevoerd. Het betreft een onderzoek waarbij het doel is het vaststellen van de materiële betrouwbaarheid van de uitkomsten van de GIS. Hierna zal dit verder worden uitgewerkt. Verder wordt in Richtlijn 621 aangegeven dat de actuaris bij zijn oordeelsvorming rekening houdt met het oordeel van de accountant over de bij de waardering van de verzekeringsverplichtingen/pensioenverplichtingen gehanteerde basisgegevens en uitgangspunten. De EDP-auditor zal het normenkader voor zijn onderzoek derhalve dienen af te leiden van de inschattingen van de accountant ten aanzien van de noodzakelijke administratieve organisatie en internecontrolemaatregelen en de fouttoleranties ten aanzien van de uitkomsten van de GIS. Naar analogie van Richtlijn 621 stelt de EDP-auditor de informatie, op grond waarvan hij tot zijn oordeel is gekomen, aan de accountant ter beschikking teneinde deze in staat te stellen tot een zelfstandig oordeel te komen over de verantwoording van de gecontroleerde organisatie. Hierbij valt te denken aan:

* het normenkader voor de noodzakelijke administratieve organisatie en internecontrolemaatregelen ten aanzien van de te onderscheiden processen afgeleid van de risicoanalyse (gebaseerd op de inschatting van het inherente risico en internecontrolerisico en de fouttoleranties in de jaarrekening);
* de beschrijving van de opzet van de general ICT controls en een oordeel over de toereikendheid daarvan;
* de functionele beschrijving van de opzet van de gecontroleerde systemen met daarin opgenomen de aanwezige toepassingscontroles;
* de beschrijving van het datamodel binnen de GIS en dataflow door de GIS;
* de beschrijving van de onderzochte rekenregels binnen de GIS;
* de weergave van de uitgevoerde controlewerkzaamheden gericht op de opzet, het bestaan en de werking van procedures binnen de automatiseringsorganisatie en de opzet en het bestaan van toepassingscontroles;
* de strekking van het oordeel van de EDP-auditor gebaseerd op de uitgevoerde werkzaamheden.

De accountant en de EDP-auditor overleggen ten slotte over de resultaten van hun werkzaamheden en de gevolgen daarvan voor de af te geven verklaring.

Positionering EDP-audit in proces van totstandkoming jaarrekening

De jaarrekening komt doorgaans tot stand in twee fasen ([Frie91]). In de eerste fase vindt registratie van transacties in de bedrijfsprocessen plaats ondersteund door GIS. Aan het einde van deze fase wordt binnen de financiële administratie een saldibalans opgemaakt. In de tweede fase worden handmatig journaalposten geboekt voor onder andere de schattingsposten in de jaarrekening zoals voorzieningen. Tot slot zal de jaarrekening opgesteld worden als resultante van saldibalans plus voorafgaande journaalposten. De tweede fase is doorgaans niet omgeven met een adequaat stelsel van maatregelen van interne controle. De voorafgaande journaalposten bestaan doorgaans uit niet-routinematige posten. De accountant zal de tweede fase derhalve doorgaans gegevensgericht controleren. De EDP-auditor zal hierbij in het algemeen geen rol van betekenis spelen. (Bij waarderingsvraagstukken rondom IT en informatiesystemen en systemen in ontwikkeling speelt hij mogelijk wel een rol.) De rol van de EDP-auditor zal zich derhalve beperken tot het vaststellen van de betrouwbaarheid (juist-

heid, tijdigheid en volledigheid) van de gegevens op de saldibalans. Een dergelijk onderzoek van de EDP-auditor zal zich richten op de initiatie van transacties (invoer in GIS), de verwerking in de GIS alsmede de uitvoer op de saldibalans.

Bij het onderzoek naar de betrouwbaarheid van de gegevens op de saldibalans spelen voor de EDP-auditor de volgende beweringsaspecten een rol: volledigheid, bestaan en accuratesse van de gegevens. Ten aanzien van de beweringsaspecten waardering, presentatie en toelichting (het traject na de totstandkoming van de saldibalans) zal de accountant geen ondersteuning van de EDP-auditor kunnen verkrijgen vanwege enerzijds het ontbreken van een adequate organisatie en anderzijds het subjectieve gehalte van de schattingen, waarbij de vakkundige oordeelsvorming van de accountant noodzakelijk is. (In de praktijk blijkt de EDP-auditor een goed klankbord te kunnen zijn op het gebied van eerdergenoemde waarderingsvraagstukken met betrekking tot IT en systemen.) Eigendom wordt doorgaans op andere wijze dan door middel van systeemgerichte controles vastgesteld.

Objecten van onderzoek bij EDP-audit in kader van controle jaarrekening

Het management van een organisatie is verantwoordelijk voor de realisering van de organisatiedoelstellingen. Dit artikel richt zich op de werkzaamheden van de EDP-auditor bij de beoordeling van de betrouwbaarheid van de totstandkoming van de saldibalans. Teneinde de realisering van een betrouwbare saldibalans te beheersen zal een cyclus van het sturen van de activiteiten en het meten van de resultaten van de activiteiten noodzakelijk zijn voor het initiëren en het uitvoeren van bijsturingsacties. Ten aanzien van de geautomatiseerde gegevensverwerking geldt hetzelfde beheersingsprincipe ([Donk95]). De realisering van de geformuleerde doelstellingen (gekoppeld aan de te beoordelen kwaliteitsaspecten) zal beheerst dienen te worden.
De betrouwbaarheid van (de uitkomsten van) een GIS wordt grotendeels bepaald door computercontroles met een algemeen karakter, de general ICT controls, en computercontroles die zich richten op de werking van een specifieke applicatie, de toepassingscontroles ([Koed96]). General ICT controls hebben invloed op het inherente risico en het internecontrolerisico. Toepassingscontroles hebben invloed op het internecontrolerisico. De EDP-auditor zal de deugdelijke grondslag aan deze controles dienen te ontlenen.

General ICT controls

General ICT controls moeten worden onderzocht per IT-infrastructuur. IT-infrastructuur kan worden gedefinieerd als het geheel van hardware, software, computergerelateerde communicatiefaciliteiten, documentatie en vaardigheden die vereist zijn ter ondersteuning van IT-diensten. Dit houdt in dat elke afzonderlijke IT-infrastructuur apart beoordeeld dient te worden.

Vanuit de controle van de jaarrekening wordt veelal het volgende onderscheid in general ICT controls gemaakt ([Munc95]):
* beleid en management;
* functiescheidingen;
* logische toegangsbeveiliging;
* fysieke toegangsbeveiliging;
* systeemontwikkeling en onderhoudsprocedures (change management);
* continuïteit;
* systeembeheerprocedures en rekencentrumprocedures;
* gebruikerssatisfactie.

Ten aanzien van afzonderlijke IT-infrastructuren kunnen verschillende eisen gesteld worden. De eisen worden gesteld vanuit de wijze van beheersing van de bedrijfsprocessen en de applicaties die de bedrijfsprocessen ondersteunen. Er zijn twee manieren waarop de processen, waaronder de gegevensverwerkende, beheerst worden:
* Gebruikers steunen op het stelsel van administratieve organisatie en interne controle binnen de automatisering(sorganisatie).
* Gebruikers steunen niet op het stelsel van administratieve organisatie en interne controle binnen de automatisering(sorganisatie).

In het laatste geval zal binnen de gebruikersorganisatie een stelsel van compenserende maatregelen van interne controle aangebracht moeten zijn, zodat onder andere de betrouwbaarheid van de geautomatiseerde gegevensverwerking beheerst wordt.

Niet alle IT-infrastructuren behoeven derhalve aan dezelfde eisen onderworpen te zijn. Bij SFNB zal voor nagenoeg alle bedrijfsprocessen sprake (dienen te) zijn van een situatie waarin wordt gesteund op het stelsel van administratieve organisatie en interne controle binnen de automatisering(sorganisatie). Gebruikers, er zijn er bij SFNB slechts weinigen, controleren de invoer niet zelfstandig op betrouwbaarheid (dit kunnen zij waarschijnlijk ook niet), zij laten deze controles over aan de applicaties en de automatiseringsorganisatie. Indien het management een beheerste (controlled) omgeving wenst, en dat is op zijn minst gezegd verstandig, dan zullen general ICT controls van een dusdanige opzet moeten zijn, dat gewaarborgd is dat de GIS op een betrouwbare wijze de gegevens verwerken en dat de geprogrammeerde toepassingscontroles juist worden uitgevoerd.
Indien goed opgezet en geïmplementeerd hebben general ICT controls een belangrijke invloed op de effectiviteit van de automatiseringsorganisatie en haar functies en waarborgen dat de geautomatiseerde gegevensverwerking in een beheerste omgeving plaatsvindt ([IIAR91]). De general ICT controls vormen derhalve de basis voor de kwaliteit van de toepassingscontroles.

Toepassingscontroles

Toepassingscontroles zijn gericht op de beheersing van de betrouwbaarheid van ([Jenk92])
* de invoer in de GIS. Invoercontroles waarborgen de volledige en juiste vastlegging van geautoriseerde trans-

acties en identificeren geweigerde, uitgestelde en dubbele invoer.
* de gegevensverwerking in en door de GIS. Controles op de verwerking waarborgen de volledige en juiste verwerking van geautoriseerde transacties.
* de uitvoer door de GIS. Uitvoercontroles waarborgen dat een volledige en juiste audit trail van de uitkomsten van de verwerking wordt gerapporteerd aan de juiste individuen voor controledoeleinden.

Voorbeelden van toepassingscontroles zijn:
* logische toegangs- en autorisatiecontroles binnen de applicaties;
* waarschijnlijkheids- en redelijkheidscontroles;
* bestaanscontroles;
* verbandscontroles;
* integriteits- en aansluitingscontroles (subadministraties en netwerk van controletotalen);
* juistheidscontroles;
* volledigheidscontroles.

Opgemerkt wordt dat naast toepassingscontroles ook de rekenregels binnen de applicaties op een juiste wijze dienen te zijn geprogrammeerd voor een betrouwbare gegevensverwerking door GIS.

Op basis van een risicoanalyse en afhankelijkheidsanalyse brengt het management van een organisatie het stelsel van beheersmaatregelen aan binnen de applicaties en automatiseringsorganisatie alsmede binnen de gebruikersorganisatie. De EDP-auditor zal de toepassingscontroles dienen te onderzoeken teneinde vast te stellen dat de beheersing van de betrouwbaarheid van de regelkring in de systemen (vanuit management-controloptiek) adequaat is.

Toepassingscontroles kunnen in de applicaties zijn geprogrammeerd, maar kunnen ook door de gebruikers handmatig worden uitgevoerd. Geprogrammeerde controles kunnen leiden tot gebruikerscontroles, bijvoorbeeld bij exception reports (uitzonderingsrapportages), die door de gebruikers verder zullen moeten worden afgehandeld.

Samenhang general ICT controls en toepassingscontroles

De samenhang tussen de general ICT controls en toepassingscontroles in het kader van de controle van de jaarrekening kan als afgebeeld in figuur 1 worden weergegeven.

Zoals uit deze figuur naar voren komt zal, indien in de controle wordt gesteund op toepassingscontroles, de voortdurende juiste werking van general ICT controls moeten worden gecontroleerd. Hiervoor is reeds gesteld dat de general ICT controls het fundament vormen voor de juiste werking van de toepassingscontroles, waarbij met name change management belangrijk is. Het onderzoek naar de kwaliteit van de general ICT controls zal derhalve ieder jaar moeten plaatsvinden. Indien blijkt dat de kwaliteit van de general ICT controls ontoereikend is, zal bij de controle van de jaarrekening geen gebruik gemaakt kunnen worden van de EDP-controles (general ICT controls en toepassingscontroles) en zal inderdaad de reeds hiervoor weergegeven 'audit around the computer' noodzakelijk zijn. In de casus SFNB zal dit betekenen dat geen goedkeurende verklaring afgegeven kan worden vanwege het ontbreken van voldoende alternatieve controlemiddelen.

De EDP-audits op de geprogrammeerde toepassingscontroles zullen moeten plaatsvinden bij implementatie van nieuwe GIS. Indien systemen stabiel zijn en niet verder worden ontwikkeld, zal na de nulmeting geen noodzaak bestaan voor het verrichten van een onderzoek naar de geprogrammeerde toepassingscontroles. Overigens worden hierbij adequate change-managementprocedures (organisatie van de systeemontwikkeling en het onderhoud) als voorwaarde gesteld. Indien de GIS worden gewijzigd of vernieuwd zal altijd een (her)beoordeling van de juiste opzet en het bestaan van toepassingscontroles moeten plaatsvinden. Dit kan worden geïnitieerd vanuit de beoordeling van de change-managementprocedures. De door de gebruikers uitgevoerde toepassingscontroles zullen wel dienen te worden onderzocht op voortdurende juiste werking. In dit artikel wordt hiervan op een enkele uitzondering na geabstraheerd, vanwege het feit dat het artikel zich richt op organisaties die in hoge mate zijn geautomatiseerd.

Samenvatting objecten van onderzoek

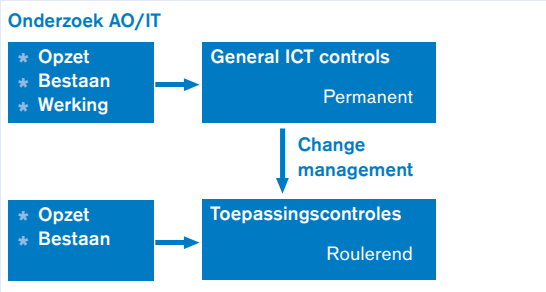
Samenvattend kunnen de volgende objecten van onderzoek van de EDP-audit worden genoemd: general ICT controls en toepassingscontroles: invoercontroles, verwerkingscontroles en uitvoercontroles. Ten aanzien van general ICT controls zijn met name van belang (omschreven in terminologie van de accountantscontrole): functiescheiding, logische toegangsbeveiliging, change-management- en systeembeheerprocedures en rekencentrumprocedures. Al deze controles moeten ervoor zorgen dat de gegevens op de saldibalans betrouwbaar zijn.

Aanpak van de EDP-audit

Voorafgaand aan de beschrijving van de aanpak zelf worden eerst de randvoorwaarden geformuleerd.

Randvoorwaarden voor audit

Alvorens de EDP-auditor een oordeel afgeeft bij een post op de saldibalans zal hij een deugdelijke grondslag dienen te verkrijgen. Ten aanzien van het verkrijgen van een deugdelijke grondslag zijn de volgende randvoorwaarden van toepassing:



Figuur 1. Samenhang onderzoek general ICT controls en toepassingscontroles.

* De kwaliteit van de controles moet objectief meetbaar zijn.
* De controlemethoden en -technieken moeten voldoende controle-informatie verstrekken.
* De uitkomsten van het onderzoek naar de kwaliteit van de controles moeten (in bepaalde mate) vertaalbaar zijn naar de kwantitatieve normen van de accountantscontrole.

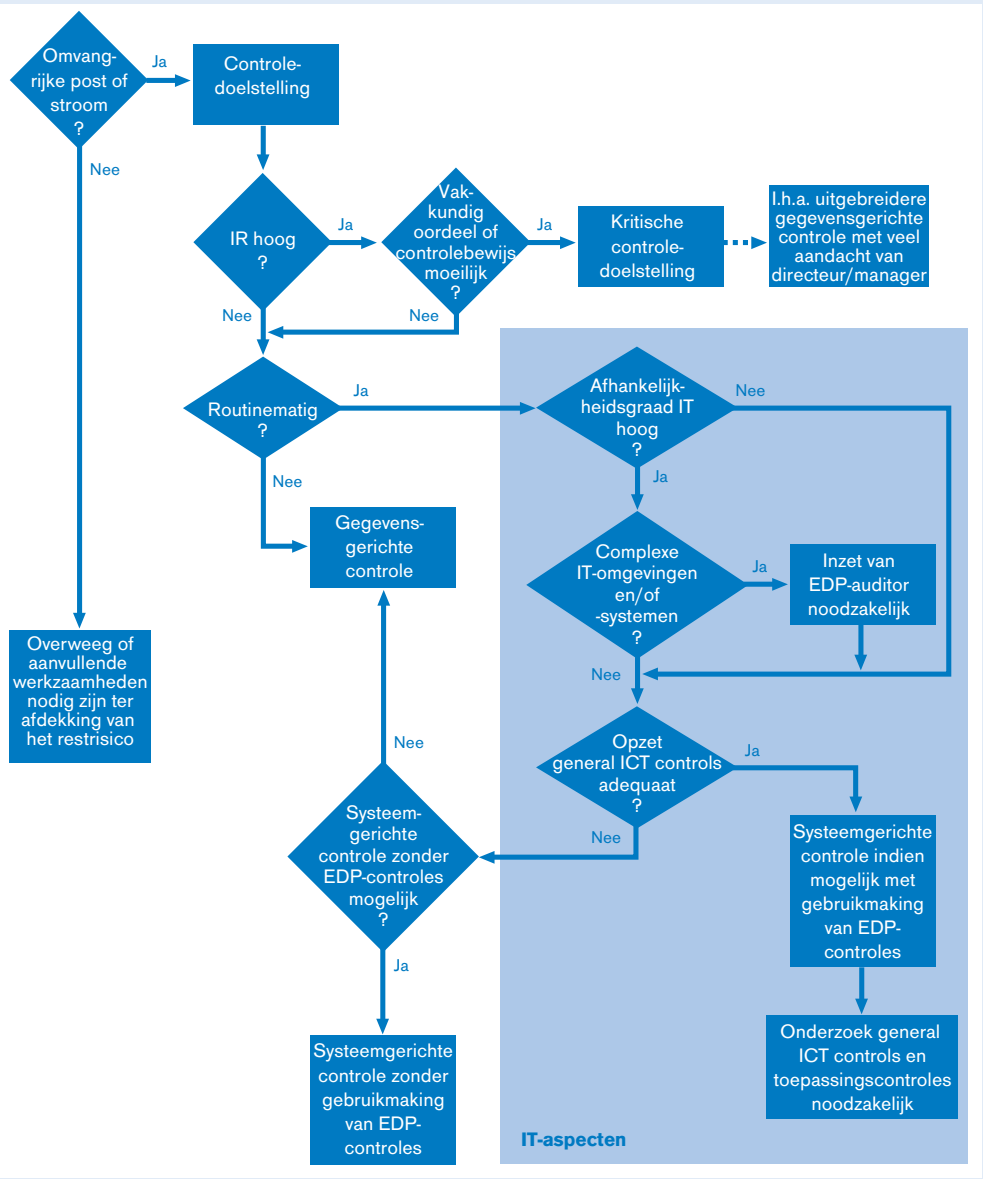
Bij de beoordeling van de uitkomsten van de uitvoering van de audit moet door de EDP-auditor getoetst worden of aan deze randvoorwaarden is voldaan.

Fasen en onderdelen van de EDP-audit

De uitvoering van de accountantscontrole is doorgaans op de volgende wijze gefaseerd: strategie, planning, uitvoering, afsluitende beoordeling, rapportage en evaluatie. Ten behoeve van de effectiviteit (het bijdragen van controle-informatie) en de efficiency van de EDP-audit is het noodzakelijk dat de EDP-auditor zijn werkzaamheden afstemt op de controleaanpak, zoals deze door de accountant wordt geselecteerd. Met name de risicoinschatting ten aanzien van het inherente risico en het internecontrolerisico alsmede de maatstaf voor de materialiteit van posten in de saldibalans zijn van belang.

Bij de EDP-audit van SFNB zal dit een ander karakter krijgen vanwege de verregaande automatisering. In dit artikel, waarin wordt gerefereerd aan de casus van SFNB, is de inzet van de EDP-auditor, die nu het merendeel van de controlewerkzaamheden uitvoert ten behoeve van het vaststellen van de betrouwbaarheid van de gegevens op de saldibalans, vooral van belang in de eerste vier fasen van het controleproces.

In figuur 2 worden de te volgen beslissingsmomenten in het controleproces weergegeven welke de controleaanpak bepalen; hierbij zijn de vraagstukken die direct een relatie hebben met de IT in een blauw kader weergege-



Figuur 2. Beslissingsboom bepaling controle-aanpak.

ven. Deze beslissingsboom is afgeleid van de KPMG Audit Service methodiek ([KPMG94]). Het schema opent met de vraag of de betreffende post of stroom in de jaarrekening omvangrijk is. Gezien het feit dat de posten en stromen voortkomen uit bedrijfsprocessen is het met het oog op de efficiency raadzaam deze beslissingsboom per bedrijfsproces (dus een bundeling van posten en stromen, die het bedrijfsproces genereert) door te lopen, omdat een bedrijfsproces veelal door één informatiesysteem wordt ondersteund, en elk systeem derhalve in de EDP-audit als afzonderlijk onderdeel onderzocht wordt.

Zoals hiervoor is gesteld, richt de EDP-auditor zich bij het onderzoek naar de betrouwbaarheid van de posten in de saldibalans op de general ICT controls en de beheersingsmaatregelen omtrent de invoer in, de verwerking in en de uitvoer van gegevens uit de GIS (toepassingscontroles). In de strategie- en planningsfase zullen de opzet, het bestaan en de werking van de general ICT controls alsmede de opzet van de toepassingscontroles worden onderzocht. Het onderzoek naar de voortdurende juiste werking van de general ICT controls kan pas worden afgerond op balansdatum, dus als het boekjaar is afgesloten. Het bestaan van toepassingscontroles wordt vastgesteld hetzij reeds in de planningsfase hetzij in de uitvoeringsfase. De rapportage van de EDP-auditor vindt plaats in de uitvoeringsfase.

Op basis van het bovenstaande kunnen ten aanzien van de EDP-audit de in tabel 1 genoemde onderdelen worden onderscheiden.

Inzicht verkrijgen in processen en systemen

Inzicht in processen en systemen is noodzakelijk voor het plannen van de noodzakelijke werkzaamheden in de EDP-audit. Er zal inzicht moeten worden verkregen in de onderstaande aspecten:
* de primaire bedrijfsprocessen en bijbehorende informatiestromen en -bestanden;
* het karakter per bedrijfsproces (sturend of ondersteunend, routinematig of niet-routinematig);
* welke bedrijfsprocessen belangrijk/kritisch zijn voor de cliënt;
* welke risico's verbonden zijn aan de belangrijke/kritische bedrijfsprocessen;
* welke geautomatiseerde systemen de belangrijke/kritische bedrijfsprocessen ondersteunen en in hoeverre de organisatie afhankelijk is van de IT;
* welke IT wordt gebruikt;
* het profiel van de automatiseringsorganisatie;
* de mate van betrokkenheid van gebruikers bij IT-ontwikkelingen.

Hierbij kan gebruik worden gemaakt van beschrijvingen van de processen en de administratieve organisatie en interne controle alsmede functie- en taakbeschrijvingen. Tevens kunnen indien noodzakelijk inlichtingen worden gevraagd aan de gecontroleerde (interviews) ten behoeve van het in kaart brengen van bovenstaande aspecten. Hulpmiddelen voor de vastleggingen van een en ander kunnen worden gevonden in schematechnieken en matrices waarin processen, functies en taken en bevoegdheden met elkaar in relatie worden gebracht.

Het in kaart brengen van bovenstaande (IT-)aspecten wordt doorgaans in samenwerking met de accountant uitgevoerd. Hiermee wordt bereikt dat in het vervolg van het onderzoek duidelijk is dat bepaalde aspecten diepgaander worden beoordeeld (de kritische IT-infrastructuur en GIS) en bepaalde aspecten minder diepgaand of in het geheel niet. Deze aspecten zullen in de planningsfase worden uitgewerkt, waarna de controleaanpak afgestemd kan worden op de uitkomsten van dit onderzoek.

Het vaststellen van de afhankelijkheid is in dit artikel gericht op betrouwbaarheid. Van de eisen ten aanzien van beschikbaarheid, effectiviteit, wettelijke bepalingen en brancherichtlijnen wordt in dit artikel geabstraheerd. De mate van afhankelijkheid geeft een indicatie voor het belang van de beheersingsmaatregelen gericht op de betrouwbaarheid. De vaststelling van de afhankelijkheid ten aanzien van het kwaliteitsaspect betrouwbaarheid komt tot stand nadat de procesanalyse is uitgevoerd. De EDP-auditor vormt zich zelfstandig een oordeel over de afhankelijkheid en zal dit afstemmen met het management van de gecontroleerde organisatie en met de accountant.

Basis voor normen voor EDP-audit

De EDP-auditor zal bij de uitvoering van de audit op de betrouwbaarheid van de gegevens op de saldibalans, zijnde de output van GIS, de normen in acht dienen te nemen die worden gesteld door de accountant. De accountant is eindverantwoordelijke voor de af te geven accountantsverklaring en zal de eisen die aan de betrouwbaarheid van de gegevens van de saldibalans worden gesteld, formuleren (de controletolerantie). De controletolerantie wordt vervolgens door de accountant verdeeld over de posten in de jaarrekening (standen en stromen); de verdeelde tolerantie wordt omschreven als evaluatietolerantie ([Aren91]).
Daarnaast baseert de accountant zijn controleaanpak mede op de inschatting van het inherente risico en het internecontrolerisico. Dit is van belang voor het onderzoek naar de general ICT controls en toepassingscontroles. Hiervoor is reeds aangegeven dat de keuze systeemgericht te controleren met gebruikmaking van de controles in de automatisering mede afhankelijk is van

Tabel 1. Fasen en onderdelen van de EDP-audit.

Fase	Onderdeel onderzoek
Strategie/planning	Inzicht verkrijgen in processen en systemen welke posten in de jaarrekening genereren, bepalen van afhankelijkheidsgraad van IT en uitvoeren van risicoanalyse op de processen
Strategie/planning	Normen formuleren ten aanzien van de te onderzoeken general ICT controls en toepassingscontroles
Planning	Beoordelen van general ICT controls en evalueren uitkomsten voor de controleaanpak
Planning/uitvoering	In kaart brengen en beoordelen van aanwezige stelsel van beheersingsmaatregelen op de juiste invoer, verwerking, uitvoer en bewaring van gegevens (beoordelen van toepassingscontroles) en evalueren van de uitkomsten van het onderzoek voor de betrouwbaarheid van de gegevens op de saldibalans
Planning/uitvoering	Rapporteren aan accountant

het beheersingsconcept van het management (het al dan niet steunen op maatregelen van interne controle in de automatisering(sorganisatie)).
De EDP-auditor zal zijn audit richten op de general ICT controls en de toepassingscontroles, welke op basis van een risicoanalyse en afhankelijkheidsanalyse door het management van de gecontroleerde organisatie zijn geïmplementeerd.

Normen voor general ICT controls
De normen die gesteld worden ten aanzien van de general ICT controls zijn afhankelijk van enerzijds het inherente risico als zodanig en anderzijds de inschatting ('waardering' in het risicoanalysemodel) van het internecontrolerisico door de accountant. Indien de accountant bij de controle van de betrouwbaarheid van een post in de jaarrekening wenst te steunen of zelfs moet steunen (zie casus SFNB) op de administratieve organisatie en interne controle, waarbij gebruikgemaakt wordt of zelfs moet worden (zie casus SFNB) van computercontroles, dan zullen de (kwaliteits)normen ten aanzien van de general ICT controls ten aanzien van de betrokken IT-infrastructuur op een hoger niveau liggen dan in het geval dat de accountant bij de controle geen gebruik maakt van de computercontroles. Daarnaast zal door de accountant een afweging gemaakt worden omtrent de mate van toepassing van gegevensgerichte maatregelen om het detectierisico af te dekken. Bij onvoldoende mogelijkheden voor gegevensgerichte maatregelen (waaronder cijferanalyses en detailcontroles) betekent dit dat de normen ten aanzien van het internecontrolerisico op een hoger niveau zullen liggen (zie casus SFNB), immers het internecontrolerisico zal lager dienen te zijn om het accountantscontrolerisico op een acceptabel niveau te krijgen.

De normen van de EDP-auditor dienen te zijn afgeleid van de normen voor de jaarrekeningcontrole.

Er is een aantal normenkaders geformuleerd waaraan bij de uitvoering van de EDP-audit kan worden gerefereerd. Te noemen zijn onder andere: CobIT, ITIL, Code voor Informatiebeveiliging, NIVRA-geschriften in de serie Automatisering en controle en NIVRA-studierapport 34. Vooraf is in de risicoanalyse van de accountant aangegeven welke norm ten aanzien van het inherente risico en het internecontrolerisico geldt. Op basis van deze inschatting én van vakkundige oordeelsvorming maakt de EDP-auditor een schatting van het minimaal noodzakelijke niveau van de general ICT controls.

Normen voor toepassingscontroles
De normen die gesteld worden ten aanzien van de toepassingscontroles zijn enerzijds afhankelijk van de inherente risico's in de bedrijfsprocessen (wat kan er zoal fout gaan in de uitvoering van de bedrijfsactiviteiten) en anderzijds afhankelijk van de inschatting van het internecontrolerisico en van de controletolerantie en evaluatietolerantie (foutenkans die niet wordt afgedekt door toepassingscontroles) door de accountant. Hierbij geldt hetzelfde betoog als bij de general ICT controls.
De normen ten aanzien van toepassingscontroles zullen specifiek per bedrijfsproces dienen te worden bepaald op basis van de risicoanalyse en gestelde controletolerantie en evaluatietolerantie.

De toepassingscontroles zijn specifiek gericht op de betrouwbaarheid van de posten in de saldibalans. De controletolerantie en evaluatietolerantie per post in de saldibalans zijn kwantitatief van aard. De controletolerantie en evaluatietolerantie kunnen derhalve worden gekwalificeerd als maatlat, waartegen de werkelijkheid kan worden afgemeten. De toepassingscontroles dienen ervoor zorg te dragen dat geen fouten in de posten op de saldibalans groter dan de controletolerantie en evaluatietolerantie voorkomen. Dit betekent dat de toegestane fout per transactie vermenigvuldigd met het aantal transacties onder de gestelde toleranties dient te blijven.

Conclusies hanteren van normen
Geconcludeerd wordt dat de normen die gesteld worden aan de general ICT controls en de toepassingscontroles, afhankelijk zijn van:
* het inherente risico;
* de door de accountant gekozen controleaanpak, die de inschatting ('waardering' in het risicoanalysemodel) van het internecontrolerisico bepaalt. Het wel of niet toepassen van gegevensgerichte controlemaatregelen beïnvloedt de eis ten aanzien van het internecontrolerisico. Dit lijkt op het eerste gezicht een omgekeerde wereld; het detectierisico bepaalt het internecontrolerisico. Het is echter mogelijk vanwege een hogere efficiency van gegevensgerichte maatregelen toch de nadruk te leggen op gegevensgerichte controles;
* de gestelde toleranties ten aanzien van posten in de jaarrekening, welke mede voortkomen uit posten op de saldibalans zijnde de uitkomsten van de GIS (met name van belang voor toepassingscontroles).

De normen zullen per specifieke situatie bepaald moeten worden.

De formulering van de normen ten aanzien van de general ICT controls en de toepassingscontroles dient te berusten op de vakkundige oordeelsvorming (veronderstelt specifieke deskundigheid) van de EDP-auditor, waarbij als randvoorwaarde is gesteld de door de accountant aangegeven controletolerantie en evaluatietolerantie per post in de jaarrekening, welke wordt gevormd door één of meer posten in de saldibalans eventueel aangevuld met voorafgaande journaalposten. De EDP-auditor dient zijn oordeelsvorming omtrent de normen ten aanzien van de general ICT controls en de toepassingscontroles te overleggen en af te stemmen met de accountant alvorens het onderzoek wordt uitgevoerd, dit om discussies bij de evaluatie van de uitkomsten van het onderzoek te voorkomen. Het verdient derhalve aanbeveling de accountant het normenkader schriftelijk te laten bevestigen.

In dit artikel wordt verder geen aandacht besteed aan de specifieke invulling van de normen.

Onderzoek general ICT controls

Het onderzoek naar de general ICT controls dient uitsluitsel te geven over de vraag of een systeemgerichte controle met gebruikmaking van EDP-controles mogelijk is.
Gezien de reikwijdte wordt in dit artikel niet inhoudelijk ingegaan op de aspecten die moeten worden onderzocht bij de genoemde onderdelen van de general ICT controls. Voor het vaststellen van de opzet en in een aantal gevallen ook tegelijkertijd het bestaan zal gebruikgemaakt worden van:
* interviews met de betrokken medewerkers in de gebruikers-, systeemontwikkelings- en verwerkings- en transportorganisatie;
* kennisnemen van procedurebeschrijvingen van de systeemontwikkelings- en verwerkings- en transportorganisatie en uitvoeren van lijncontroles;
* kennisnemen van de mogelijkheden en de toepassing van de mogelijkheden (maatregelen van interne controle) van de aanwezige besturings- en toegangsbeveiligingsprogrammatuur alsmede het databasemanagementsysteem, en vaststellen van het bestaan van de maatregelen van interne controle.

De werking van de general ICT controls wordt vastgesteld door middel van het uitvoeren van proceduretests op die aspecten/maatregelen van interne controle waaraan de controle-informatie ten behoeve van de onderbouwing van de controleaanpak (systeemgericht met gebruikmaking van EDP-controles) wordt ontleend. Hieruit kan worden afgeleid dat de werking van de general ICT controls zichtbaar moet zijn om achteraf de juiste uitvoering te kunnen vaststellen. Indien controles niet zichtbaar zijn zal geen uitspraak gedaan kunnen worden over de werking, tenzij de EDP-auditor permanent aanwezig is ter vaststelling van de werking, hetgeen een irrationele controle impliceert (zeer hoge kosten).

Evaluatie general ICT controls voor controleaanpak
De uitkomsten van het onderzoek naar de opzet, het bestaan en de werking van bovengenoemde general ICT controls zijn objectief meetbaar. De normen zijn vastgelegd in de voorgaande fase. In deze fase wordt getoetst aan de vastgelegde norm.
De EDP-auditor zal na afronding van de beoordeling van de opzet en het bestaan een tussenrapportage verstrekken aan de accountant ter onderbouwing van de controleaanpak. Na afronding van het onderzoek naar de general ICT controls (op zijn vroegst om 0.00 uur van de eerste dag van het nieuwe boekjaar) zal de EDP-auditor de accountant kunnen rapporteren over de voortdurend juiste werking van de general ICT controls gedurende het gehele boekjaar. Een voortdurend juiste werking stelt hoge eisen aan de automatiseringsorganisatie (toereikende zichtbare en verifieerbare controles).

De rapportage van de uitkomsten van het onderzoek naar de opzet van de general ICT controls zal de accountant uitsluitsel dienen te geven dat de gekozen controleaanpak (systeemgericht met gebruikmaking van EDP-controles) mogelijk is of niet. Er zal een antwoord gegeven moeten worden op de vraag of de general ICT controls adequaat zijn van opzet. Nadat de juiste opzet is vastgesteld, zal het onderzoek naar de voortdurend juiste werking worden uitgevoerd.

Indien bij het onderzoek van de general ICT controls blijkt dat een systeemgerichte controle met gebruikmaking van EDP-controles niet mogelijk is, zal de EDP-auditor hierover direct aan de accountant rapporteren. De EDP-auditor zal de (onbevredigende) uitkomst met de accountant bespreken en de gevolgen voor de controleaanpak aangeven. In de situatie van de casus van SFNB zal de conclusie luiden dat de jaarrekening van SFNB niet controleerbaar is vanwege het ontbreken van een 'adequaat' stelsel van administratieve organisatie en interne controle. De accountant zal in dit geval met redenen omkleed het management van SFNB rapporteren, dat geen goedkeurende verklaring afgegeven kan worden. In dit artikel wordt verder geabstraheerd van het probleem of sprake is van subjectieve verhindering.

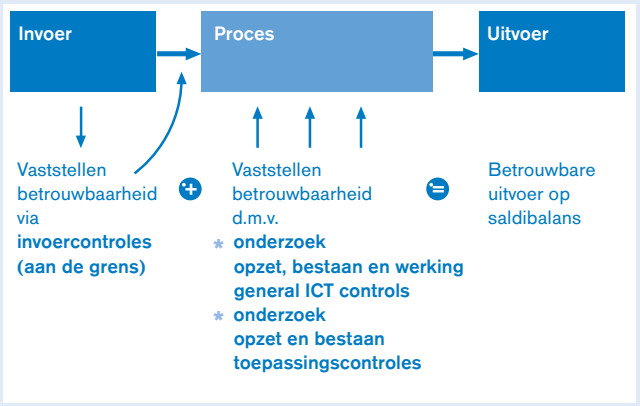
Onderzoek toepassingscontroles

Op basis van de uitgevoerde risicoanalyse en het oordeel over de opzet van de general ICT controls zal door de EDP-auditor onderzocht dienen te worden op welke wijze de beheersingsmaatregelen in de applicaties zijn aangebracht (geprogrammeerd) of op welke wijze de beheersingsmaatregelen in de gebruikersorganisatie zijn getroffen.
Hiervoor is reeds onderscheid gemaakt tussen de volgende toepassingscontroles:
* invoercontroles (inclusief autorisatiecontroles);
* verwerkingscontroles;
* uitvoercontroles.

Figuur 3 licht de plaats en het belang van toepassingscontroles nader toe.

De EDP-auditor maakt bij zijn onderzoek naar de opzet en het bestaan van de toepassingscontroles onder andere gebruik van de volgende controlemethoden en -technieken:
* kennisnemen van organigram, taken en bevoegdheden medewerkers, administratieve procedures en de daarin vervatte maatregelen van interne controle;
* kennisnemen en beoordelen van systeemdocumentatie van de GIS;
* kennisnemen en beoordelen van beschrijving informatiearchitectuur en de daarbij aangegeven eigenaren van data;
* interviews met systeemontwikkelaars/projectleider;
* interviews met (kern)gebruikers;
* kennisnemen van testrapportages (systeem- en gebruikerstests);

Figuur 3. Overzicht controleaanpak voor vaststelling betrouwbaarheid invoer.



* uitvoeren van lijncontroles van transacties door de GIS.

Het meten van de effectiviteit en de toereikendheid van de toepassingscontroles (bijdrage aan de controle-informatie voor de onderbouwing van de grondslag voor de af te geven accountantsverklaring) berust op vakkundige oordeelsvorming van de EDP-auditor. De EDP-auditor zal hiervoor over voldoende kennis van administratieve organisatie en interne controle dienen te beschikken.
Voorop staat dat de fouten die in posten op de saldibalans voorkomen, tezamen in omvang niet de gestelde controletolerantie en evaluatietolerantie per post te boven mogen gaan. De toepassingscontroles zullen dit moeten waarborgen.

Mochten bovenstaande werkzaamheden onvoldoende controle-informatie opleveren, dan zal de EDP-auditor zijn eigen werkzaamheden moeten uitbreiden. Hierbij kan gedacht worden aan het uitvoeren van eigen testwerkzaamheden en het zelfstandig controleren van de juiste werking van verbandscontroles.

Hieronder wordt een aantal aandachtspunten weergegeven ten aanzien van bovengenoemde toepassingscontroles (van gebruikerscontroles wordt geabstraheerd).

Invoercontroles
De EDP-auditor stelt vast dat de invoercontroles zekerheid geven omtrent volledigheid, juistheid en tijdigheid van de registratie van de invoer van geaccepteerde en uitgevoerde transacties.
In het in figuur 3 weergegeven schema is aangegeven dat invoercontroles dienen te bewerkstelligen, dat de registratie van de geaccepteerde en uitgevoerde transacties betrouwbaar plaatsvindt. Derhalve zal bij het onderzoek naar de toepassingscontroles de nadruk worden gelegd op invoercontroles.

Ten behoeve van het vaststellen van de volledigheid van invoer zal aan de onderstaande aspecten inhoud moeten zijn gegeven en zullen deze derhalve door de EDP-auditor moeten worden beoordeeld. De beoordeling zal zich richten op het toetsen aan de gestelde (kwantitatieve) normen, welke zijn afgeleid van de controletolerantie en evaluatietolerantie. Tezamen met de andere toepassingscontroles mogen geen fouten in de posten van de saldibalans onontdekt blijven door de GIS, welke tezamen de toleranties overschrijden. Aan de volgende aspecten zal invulling moeten zijn gegeven:
* Logginginformatie van aan de GIS aangeboden en door de GIS geaccepteerde en uitgevoerde transacties moet beschikbaar blijven.
* Alle geaccepteerde en uitgevoerde transacties zullen in een invoerbestand beschikbaar dienen te blijven als 'brondocumenten'.
* Eenmaal in de GIS ingevoerde en door de GIS geaccepteerde en uitgevoerde transacties (dus in overeenstemming met de autorisatiestructuur in de administratieve organisatie) mogen niet meer verwijderd en ongeautoriseerd gewijzigd kunnen worden.

De controles die deze aspecten afdekken, kunnen worden bestempeld als onvervangbare interne controles. Achteraf is zonder de noodzakelijke (betrouwbare) basisinformatie niet meer vast te stellen of de uitkomsten van de GIS betrouwbaar zijn weergegeven.

Als de casus SFNB hierbij betrokken wordt, zal een soort elektronisch postontvangstregistratiesysteem noodzakelijk zijn voor het vaststellen van de volledigheid van de registratie van de via Internet ontvangen geaccepteerde en uitgevoerde transacties. Indien geen zekerheid verkregen wordt omtrent de betrouwbaarheid van de registratie van geaccepteerde en uitgevoerde transacties zal de EDP-auditor zich – bijvoorbeeld door middel van verbandscontroles – geen oordeel kunnen vormen omtrent de output van de GIS en zal de accountant derhalve geen controle-informatie ontvangen, welke kan dienen als deugdelijke grondslag voor het afgeven van een goedkeurende verklaring.

De EDP-auditor zal verder invoercontroles die de juistheid en accuratesse van de (schone) invoer bewerkstelligen, beoordelen. Deze invoercontroles kunnen zijn:
* waarschijnlijkheids- en redelijkheidscontroles;
* bestaanscontroles;
* juistheidscontroles;
* volledigheidscontroles.

Tot slot zal de EDP-auditor de aanwezigheid vaststellen van controles die controleren dat alle ingevoerde transacties in het invoerbestand door de GIS zijn verwerkt.

Toegangscontroles
De toegangscontroles zijn noodzakelijk voor de beveiliging van de integriteit van data en applicaties. De EDP-auditor stelt vast dat de toegangscontroles in de applicaties op een adequate wijze zijn ingevuld. Hiertoe zal hij gebruikmaken van de faciliteiten die het ontwikkeltool waarmee de GIS zijn ontwikkeld, biedt. Hij zal hierbij, indien deze aanwezig is, gebruikmaken van de functiematrix waarin gebruikers worden gekoppeld aan functies of modules. Indien deze functiematrix ontbreekt zal de EDP-auditor op een alternatieve wijze de inrichting van de toegangscontrole dienen vast te stellen. Bij de beoordeling van de general ICT controls is reeds invulling gegeven aan de logische toegangsbeveiliging tot de data en systemen in het algemeen.

De norm (maatlat) voor de beoordeling van de toegangscontroles is zodanig dat niet afgeweken mag worden van de bevoegdhedenstructuur, zoals deze is vastgelegd in de administratieve organisatie. Er dient derhalve minimaal aan deze norm te zijn voldaan. Functiescheidingen mogen niet worden doorbroken in de applicaties.

Verwerkingscontroles
De verwerkingscontroles moeten de betrouwbaarheid van de verwerking van transacties waarborgen. De EDP-auditor stelt vast dat de geprogrammeerde maatregelen in de GIS een adequaat stelsel vormen. Hierbij zal met name gebruik kunnen worden gemaakt van verbandscontroles (netwerk van controletotalen), audit trails en foutverslagen, welke geproduceerd worden van tijdens de verwerking geweigerde transacties. Verbandscontroles (vergelijking van output met input in totalen) dienen te bewerkstelligen dat geen mutaties verloren gaan tijdens de verwerking. Tevens kan gebruikgemaakt worden

van een vergelijking van de telling van het aantal transacties aangeboden ter verwerking en het aantal verwerkte transacties met eventueel het aantal geweigerde transacties in een wachtbestand.

Van alle fouten die tijdens de verwerking zijn opgetreden, zullen uitzonderingsrapportages uit de GIS verkregen dienen te worden. De uitzonderingsrapportages zullen door de gebruikers afgewerkt moeten worden. Deze uitzonderingsrapportages zullen doorlopend genummerd en na afwerking op een centrale plaats gearchiveerd dienen te worden, zodat van deze maatregelen van interne controle het bestaan en de juiste werking vastgesteld kunnen worden. De handmatige correctieprocedures rondom de verwerking zullen door de EDP-auditor worden beoordeeld.

De interfaces tussen de diverse GIS (indien geen sprake is van één geïntegreerd GIS) zullen door de EDP-auditor op betrouwbaarheid (en controleerbaarheid) dienen te worden beoordeeld.

De norm (maatlat) voor bovenstaande beoordelingen wordt gevormd door de controletolerantie en evaluatietolerantie, die aan de posten in de saldibalans zijn toegekend. De fouten (het totaalbedrag aan fouten) die door de verwerkingscontroles niet worden ontdekt (tezamen met de overige toepassingscontroles), mogen in omvang de gestelde toleranties niet overschrijden.

Naast de genoemde werkzaamheden gericht op het vaststellen van de toereikendheid van de verwerkingscontroles zal specifiek aandacht dienen te worden geschonken aan memoriaalboekingen in de financiële administratie. Memoriaalboekingen kunnen worden gekarakteriseerd als niet-routinematig. Omdat een memoriaalboeking een post in de saldibalans kan raken welke systeemgericht wordt gecontroleerd, is onderzoek naar de juistheid en autorisatie van memoriaalboekingen echter wel noodzakelijk. Een memoriaalboeking kan doorbreking van functiescheiding en bevoegdheden, zoals deze in de organisatie en in de GIS aanwezig zijn, inhouden. De memoriaalboekingen worden doorgaans door de financiële administratie direct in het grootboek verwerkt. Met behulp van bestandsanalyse zullen deze transacties op een efficiënte wijze kunnen worden achterhaald en vervolgens op juistheid (en autorisatie) worden gecontroleerd (eventueel uit te voeren door de accountant).

Uitvoercontroles

Uitvoercontroles dienen te waarborgen dat alle verwerkte transacties worden bijgewerkt in de (uitvoer-) bestanden. Het databasemanagementsysteem zal hiertoe functionaliteiten kunnen bieden. Indien de verwerking onjuist is verlopen of indien de verwerking is vastgelopen, zal teruggegaan moeten kunnen worden naar de situatie voor de transactie (zogenaamde rollback); de (referentiële) integriteit van de bestanden dient te zijn gewaarborgd. Verder kan gebruikgemaakt worden van verbandscontroles zoals weergegeven bij de verwerkingscontroles.

Voor de norm voor de uitvoercontroles kan worden verwezen naar de andere toepassingscontroles. Tezamen met de andere toepassingscontroles mogen geen fouten in de posten van de saldibalans voorkomen die de toleranties overschrijden.

Rekenregels

Rekenregels binnen de applicaties van de GIS vormen het hart van de gegevensverwerking. Met behulp van de rekenregels worden gegevens omgezet van invoer naar uitvoer. Het zal derhalve duidelijk zijn dat de EDP-auditor geen uitspraak kan doen omtrent de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans indien hij de rekenregels niet heeft beoordeeld op juistheid. De beoordeling van de rekenregels vergt kennis van de bedrijfseconomie (het berekenen van de financiële consequenties van transacties) en de bedrijfsadministratie (wijze van verslaglegging van de financiële consequenties in de financiële administratie) en indien relevant de financiële rekenkunde en levensverzekeringswiskunde.

Mogelijkerwijs kan de accountant hierbij ondersteuning bieden. De EDP-auditor zal zich zelfstandig een oordeel moeten vormen omtrent de juistheid van de rekenregels. Indien hij hiertoe niet in staat is zal hij geen uitspraak kunnen doen omtrent de uitkomsten van de GIS. In de GBRE zijn geen bepalingen opgenomen omtrent de samenwerking met andere deskundigen voor deelonderzoeken, zoals het onderzoeken van rekenregels. Er wordt derhalve aansluiting gezocht bij de Richtlijnen voor de Accountantscontrole (Richtlijn 620).

Evaluatie/conclusies onderzoek toepassingscontroles voor betrouwbaarheid saldibalans

De kwaliteit van de toepassingscontroles (met name invoercontroles zijn van belang) en de juistheid van de rekenregels is meetbaar. De toetsing van de kwaliteit van de toepassingscontroles, die dienen te waarborgen dat aan de kwantitatieve normen die gelden voor fouten in posten op de saldibalans is voldaan, is mogelijk. Indien is vastgesteld dat het opgezette stelsel (samenstel) van toepassingscontroles adequaat is en rekenregels juist zijn geprogrammeerd, indien daarnaast is vastgesteld dat de controles bestaan (juist zijn geprogrammeerd en gebruikerscontroles juist worden uitgevoerd) en indien deze controles geplaatst zijn in een betrouwbare (stabiele) geautomatiseerde omgeving (general ICT controls zijn adequaat), dan bestaat voldoende zekerheid omtrent de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans.
Overigens wordt nogmaals benadrukt dat de beoordeling van de toereikendheid van de general ICT controls en toepassingscontroles berust op vakkundige oordeelsvorming van de EDP-auditor; de normen zijn met een zekere mate van subjectiviteit bepaald. Aangegeven is dat de normen vooraf afgestemd moeten worden met de accountant. Het gaat om de mate van acceptabel restrisico (ontdekkingsrisico), hetgeen is vastgelegd in de normen zoals hiervoor is omschreven.
De EDP-auditor zal de uitkomsten van de controlewerkzaamheden toetsen aan de normen ten aanzien van het controlerisico, de controletolerantie en evaluatietolerantie, zoals deze door de accountant zijn gesteld, en vervolgens zijn rapportage (de mededeling) opstellen, verstrekken en toelichten aan de accountant.

De volgende oordelen van de EDP-auditor zijn mogelijk ten aanzien van het onderzoeksobject, de saldibalans ([Velt95]):

* Goedkeurend, indien geen materiële tekortkomingen in de opzet, het bestaan en de werking van de general ICT controls en de opzet en het bestaan van de toepassingscontroles zijn geconstateerd of materiële onderzoeksonzekerheden ten aanzien van deze controles zijn blijven bestaan.
* Goedkeurend met beperking, indien er sprake is van een materiële tekortkoming en/of materiële onderzoeksonzekerheid. Tekortkomingen kunnen betrekking hebben op de werking van general ICT controls en/of de opzet en het bestaan van toepassingscontroles (eventueel van werking van door gebruikers uitgevoerde toepassingscontroles).
* Oordeelonthouding. Dit oordeel zal in de praktijk overigens niet van toepassing zijn voor dit type audit. Er zal geen sprake zijn van onzekerheid. Indien een omissie is vastgesteld of indien geen zekerheid kan worden verkregen over de opzet en het bestaan van de administratieve organisatie en interne controle, dan voldoet de administratieve organisatie en interne controle niet aan de daaraan te stellen eisen: een afkeurend oordeel of oordeel met beperking zijn dan de mogelijkheden.
* Afkeurend, indien de EDP-auditor tot het oordeel is gekomen dat de general ICT controls en/of de toepassingscontroles niet voldoen aan de gestelde criteria, zodat geen zekerheid verkregen kan worden omtrent de betrouwbaarheid van de output van de GIS. Er is sprake van een combinatie van tekortkomingen van wezenlijk belang.

De accountant zal op basis van het oordeel van de EDP-auditor in staat moeten zijn, zijn oordeel over de getrouwheid van de jaarrekening (voor wat betreft de beweringsaspecten die zijn onderzocht door de EDP-auditor) te vormen. De accountant zal zich overigens zelfstandig een oordeel moeten kunnen vormen omtrent de uitkomsten van het onderzoek van de EDP-auditor.

De accountant zal zich zelfstandig een oordeel moeten vormen omtrent de uitkomsten van de EDP-audit.

In de casus SFNB heeft de accountant geen mogelijkheid voor het uitvoeren van detailcontroles zodat geen of onvoldoende controle-informatie op een alternatieve wijze kan worden verkregen (gegevensgerichte controle). Dit impliceert dat de accountant de mededeling van de EDP-auditor, onder voorbehoud dat in het traject saldibalans naar jaarrekening geen tekortkomingen worden geconstateerd, direct kan vertalen naar de accountantsverklaring. Het verdient derhalve de voorkeur de mededeling van de EDP-auditor op een soortgelijke wijze op te stellen als een accountantsverklaring.

Samenvatting

De vraagstelling binnen dit artikel heeft plaatsgevonden in het kader van het verkrijgen van controle-informatie ten behoeve van de controle van de jaarrekening van organisaties met verregaand geautomatiseerde informatiesystemen (GIS), waarbij controle met behulp van brondocumenten rondom de computer niet meer mogelijk of niet meer efficiënt is. De accountant beschikt vanuit zijn deskundigheidsgebied in deze gevallen veelal niet meer over controlemiddelen om zelfstandig tot oordeelsvorming omtrent de getrouwheid van een jaarrekening te komen. De accountant zal daarom gebruik kunnen maken van de deskundigheid van de EDP-auditor. Dit artikel geeft uitsluitsel over de vraag aan welke voorwaarden moet zijn voldaan voordat een EDP-auditor een uitspraak over de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans (object van onderzoek) kan doen in omgevingen met verregaand GIS.

De accountant zal doorgaans zelfstandig het totstandkomingstraject van saldibalans naar jaarrekening controleren vanwege het ontbreken van een adequaat stelsel van maatregelen van interne controle en de aard van de uitgevoerde journaalposten (niet-routinematig en veelal schattingsposten).
De Richtlijnen voor de Accountantscontrole schrijven voor dat de accountant altijd zelfstandig nog eigen controlewerkzaamheden dient te verrichten bij het verkrijgen van controle-informatie, hij moet altijd zelfstandig tot een oordeel komen. Vanuit het risicoanalysemodel zal de EDP-auditor met name de inschatting van het inherente en het internecontrolerisico kunnen onderbouwen door middel van het uitvoeren van een EDP-audit. De noodzaak voor de inzet van de EDP-auditor in de jaarrekeningcontrole is situatieafhankelijk, de complexiteit van de GIS en de deskundigheid van de accountant zijn hier bepalende factoren. Voorop staat, dat de accountant zich zelfstandig een oordeel kan vormen omtrent de uitkomsten van de werkzaamheden van de EDP-auditor.

De normen voor de EDP-audit op de betrouwbaarheid van de uitkomsten van de GIS op de saldibalans (verder te noemen de EDP-audit) zijn afhankelijk van de bepaling van de materialiteitsgrenzen die door de accountant zijn gesteld ten aanzien van de te controleren jaarrekening. Tevens zal het controlerisico (afhankelijk van het inherente risico en het internecontrolerisico) medebepalend zijn voor de normstelling bij de EDP-audit. De normen zullen voordat de EDP-audit wordt uitgevoerd door de EDP-auditor, worden afgestemd met de accountant. De betrouwbaarheid van (de uitkomsten van) een GIS wordt grotendeels bepaald door computercontroles met een algemeen karakter, de general ICT controls, en computercontroles die zich richten op de werking van een specifieke applicatie, toepassingscontroles. General ICT controls hebben invloed op het inherente risico en het internecontrolerisico. Toepassingscontroles hebben invloed op het internecontrolerisico. Toepassingscontroles kunnen worden onderverdeeld naar invoercontroles, toegangscontroles, verwerkingscontroles en uitvoercontroles. Daarnaast zal de juistheid van de rekenregels binnen de GIS vastgesteld moeten worden. Al deze controles dienen ervoor zorg te dragen dat de gegevens op

de saldibalans betrouwbaar zijn; de EDP-auditor zal de deugdelijke grondslag aan deze controles moeten ontlenen.
Ten aanzien van de uitvoering van de EDP-audit is een aantal randvoorwaarden van toepassing: de kwaliteit van de controles moet objectief meetbaar zijn, de methoden en technieken moeten voldoende controle-informatie verstrekken en tot slot moeten de uitkomsten van het onderzoek naar de kwaliteit van de controles (in bepaalde mate) vertaalbaar zijn naar de kwantitatieve normen van de accountantscontrole. Indien aan één of meer van deze randvoorwaarden niet voldaan is, kan geen sprake zijn van een deugdelijke grondslag voor het afgeven van een mededeling.

De aanpak van de EDP-audit kan als volgt worden weergegeven:
1 inzicht verkrijgen in processen en systemen die posten in de jaarrekening genereren, bepalen van afhankelijkheidsgraad van IT en uitvoeren van risicoanalyse op de processen;
2 normen (maatstaf voor hoeveel procent zekerheid kan worden verkregen ten aanzien van het inherente en internecontrolerisico) formuleren ten aanzien van de te onderzoeken general ICT controls en toepassingscontroles;
3 beoordelen van general ICT controls en evalueren uitkomsten voor de controleaanpak;
4 in kaart brengen en beoordelen van het aanwezige stelsel van beheersingsmaatregelen op de invoer, verwerking, uitvoer en bewaring van gegevens (beoordelen van toepassingscontroles) en evalueren van uitkomsten onderzoek voor de betrouwbaarheid van de gegevens op de saldibalans;
5 rapporteren uitkomsten van onderzoek aan accountant.

In dit onderzoek is vastgesteld dat bij de EDP-audit kan worden voldaan aan de hiervoor gestelde randvoorwaarden voor het verkrijgen van een deugdelijke grondslag voor het afgeven van een mededeling over de betrouwbaarheid van de uitkomsten van de GIS. Met name de controle op de betrouwbaarheid van de registratie van geaccepteerde en uitgevoerde transacties zal in de audit aandacht dienen te krijgen.

Conclusies

De accountant blijft eindverantwoordelijke voor het afgeven van de verklaring over de getrouwheid van de jaarrekening en zal daartoe zelfstandig controlewerkzaamheden dienen te verrichten.

Een EDP-auditor kan een uitspraak doen over de beweringen volledigheid, bestaan en accuratesse (kwaliteitsaspect: betrouwbaarheid) van één of meer posten in de saldibalans of de gehele saldibalans afhankelijk van de wijze van inrichting van de administratieve organisatie en interne controle, en van de toepassing van IT. Het object van onderzoek zal hierbij vooraf met de accountant worden afgesproken. De in de applicaties opgenomen rekenregels kunnen door de accountant worden beoordeeld op juistheid.

Er zijn in de uitvoering van de EDP-audit enkele zaken waarbij vakkundige oordeelsvorming van de EDP-auditor onontbeerlijk is. De accountant zal zich zelfstandig een oordeel moeten kunnen vormen omtrent de uitkomsten van de EDP-audit. Daarnaast kan de accountant ten aanzien van de uitvoering van de EDP-audit zekerheid ontlenen aan het feit dat de EDP-auditor als lid is ingeschreven in het Register van de Nederlandse Orde van Register EDP-Auditors (NOREA).

Het is een geruststelling dat jaarrekeningen ook in de toekomst bij voortschrijdende automatisering kunnen blijven worden gecontroleerd, mits is voldaan aan de voorwaarden die zijn gesteld ten aanzien van de administratieve organisatie en interne controle alsmede de toepassing van IT. Ongetwijfeld is hiermee de discussie over de inzet van EDP-auditors in de controle van de jaarrekening niet beëindigd; wellicht kan echter met dit artikel weer een stap worden gezet in de goede richting.

Literatuur

[Aren91]
Prof. A.A. Arens en J.K. Loebecke, *Auditing an integrated approach*, Prentice-Hall International Editions, Englewood Cliffs, 1991.

[Donk95]
Ir. J.A.M. Donkers, M. Groesz RE en ir. J.A. Verstelle RE, *Informatietechnologie, management control van de geautomatiseerde informatievoorziening*, Kluwer Bedrijfswetenschappen, 1995.

[Frie91]
Prof. dr. A.B. Frielink RA en prof. H.J. de Heer RA, *Leerboek Accountantscontrole 2A: De algemene controle, typologie accountantscontrole in het kader van de accountantscontrole*, Stenfert Kroese, Leiden-Antwerpen 1991.

[IIAR91]
The Institute of Internal Auditors Research Foundation, *Systems Auditability and Control, Module 2, Audit and Control Environment*, Altamonte Springs 1991.

[Jenk92]
B. Jenkins MA FCA, P. Cooke Bsc FCA, P. Quest MA FCA, *An Audit Approach to Computers*, The Institute of Chartered Accountants in England and Wales, Chartered Accountants' Hall, London 1992.

[Koed96]
Drs. M.J.A. Koedijk RA en W.A. de Munck RA, *System Review Services*, Compact 1996/3.

[KPMG94]
Handboek KPMG Audit Service, KPMG, Amsterdam 1994.

[Munc95]
W.A. de Munck RA, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering*, Compact 1995/3.

[NIVR96]
Koninklijk NIVRA, *Richtlijnen voor de Accountantscontrole*, Amsterdam 1996.

[Velt95]
Drs. P. Veltman RE RA, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 1995/3.