Informatietechnologie en **interne beheersing** (deel 1)

Wanneer komen de wereld van IT-audit en financial audit bij elkaar? Menigeen vraagt zich dit af [KOUT13]. IT-auditors krijgen soms het idee dat, zelfs als de informatietechnologie (IT) cruciaal is voor een klant, zij nauwelijks budget krijgen om de IT-audits die nodig zijn te kunnen uitvoeren. Financial auditors voelen zich soms gekleineerd door de hoeveelheid IT-termen die ze over zich heen krijgen. De beide delen van dit artikel zijn geschreven om de financial auditor een aantal uitgangspunten te bieden om de samenhang van onvervangbare interne beheersing en informatietechnologie onder de knie te krijgen. Het is ook geschreven om de IT-auditor kennis te laten nemen van het raamwerk waar de financial auditor zijn vragen op baseert of kan baseren.

HEIN KLOOSTERMAN EN RUUD SNOEKER

Informatietechnologie is voor veel auditors een 'mer à boire'. Dit artikel beoogt die omvangrijke hoeveelheid stof tot een aantal kernpunten terug te brengen. In dit eerste deel geven we daartoe in de volgende paragraaf een uitwerking van een aantal – doorgaans impliciete – uitgangspunten voor de interne beheersing en de relatie ervan met informatietechnologie (IT). De uitwerking is gegeven vanuit het gezichtspunt van het beroep van de controlerend accountant: hoe moet deze de interne beheersing in samenhang met de IT toetsen. Het tweede deel van die paragraaf geeft voorbeelden van maatregelen die kunnen zijn genomen.
De daarop volgende paragraaf werkt een aantal kernelementen uit die te maken hebben met de financiële controle. Ook daar geven we een kijk op de interne beheersing. Maar dan vanuit de vraag: Hoe kan een accountant vaststellen of de maatregelen van onvervangbare interne beheersing werk(t)en? Als Leitmotiv gebruiken de auteurs het 'transactiemodel'.

INTERNE BEHEERSING IT

Uitgangspunten

In grote lijnen kan IT ten behoeve van de bedrijfsvoering worden geschetst als bestaande uit IT-processen en IT-data. Zie figuur 1.

Gebruikers werken met IT-processen en daarmee ook met IT-data. Om te weten wie welke data heeft geraadpleegd, toegevoegd of gewijzigd is het nodig dat niet iedereen zonder meer alle IT-processen beschikbaar heeft en door middel van die processen alle data kan raadplegen, toevoegen, verwijderen en/of muteren. Om dit te realiseren, is er bescherming van de IT-processen en IT-data nodig. Dat is in figuur 2 weergegeven door een schil om de processen en data te tekenen.

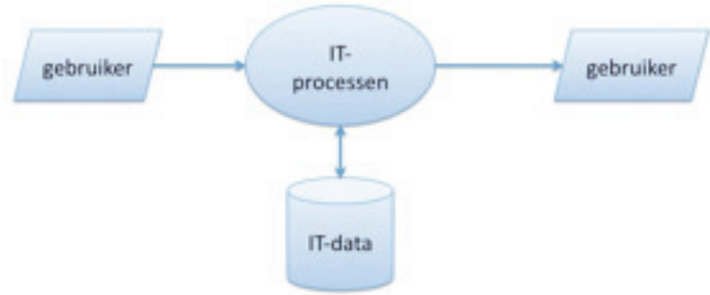
Op basis van deze twee figuren geven we een aantal uitgangspunten:

- Er is een corporate database.
- IT-processen zijn in de te beoordelen periode onveranderd gebleven.
- IT-data worden slechts toegevoegd, niet gewijzigd.
- IT-data zijn raadpleegbaar.
- Alleen geautoriseerde medewerkers kunnen data (mutaties) toevoegen.

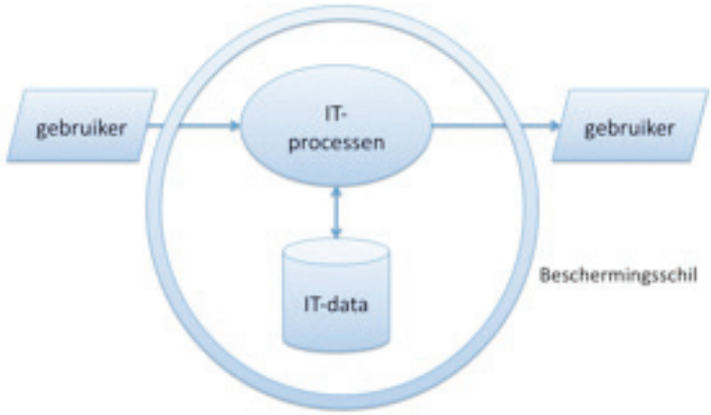
Voor de controle van de jaarrekening kan de accountant door onderzoek vaststellen of in voldoende mate is voldaan aan deze uitgangspunten; ofwel, is er sprake van een toereikende verzameling maatregelen voor de beheersing van IT-processen en IT-data?
Hierna lichten we de uitgangspunten kort toe.

Corporate database

Het uitgangspunt dat er sprake zou moeten zijn van een corporate database impliceert dat gegevens slechts één keer worden vastgelegd. Als dat niet het geval is zijn er risico's[1] zoals verlies van consistentie.
Uit onderzoek van de accountant blijkt of er inderdaad sprake is van ▶



Figuur 1: Gebruikers raadplegen data en voegen data toe



Figuur 2: Gebruikers kunnen niet ongebreideld data raadplegen of toevoegen

zo'n database dan wel dat er sprake is van doublure van gegevens.
Indien er sprake is van een ERP-systeem is er in beginsel sprake van zo'n corporate database, met eenmalige vastlegging van gegevens. Als er sprake is van zogenoemde eilandautomatisering[2] is extra aandacht nodig voor de consistentie van de data, zoals extra maatregelen rond synchronisatie en interfaces. Bij een ERP-pakket moet de consistentie door het pakket worden verzorgd.

IT-processen onveranderd

Als de IT-processen in de voorgaande perioden naar behoren werkten en gedurende de te onderzoeken periode onveranderd zijn gebleven, dan is de verwachting dat de werking over deze periode ook naar behoren is.
Zijn er wel veranderingen doorgevoerd, dan was er sprake van re-engineering waarbij bestaande dan wel nieuwe IT-data en/of IT-processen zijn betrokken. Om blijvend te kunnen voldoen aan het gewenste niveau van betrouwbaarheid en beschikbaarheid van informatie zijn maatregelen vereist in de categorie *change management*.
De accountant die de interne beheersing beoordeelt, zal vaststellen welke veranderingen zijn doorgevoerd, onder welke sturing en beheersing die wijzigingen zijn doorgevoerd en welke impact dat alles heeft op de interne beheersing.
Het is onwaarschijnlijk dat de IT-data en/of IT-processen in een periode onveranderd zijn gebleven. Behalve door functionele wijzigingen verandert de IT ook door updates van systeemsoftware en support van applicaties – waaronder de support die verband houdt met aanpassingen in systeemsoftware.

IT-data slechts toevoegen, niet wijzigen

Idealiter worden gegevens over transacties slechts toegevoegd en niet gewijzigd. Dat betekent dat wijzigingen in (semi-)permanente gegevens door het toevoegen van gegevens over de periode van geldigheid worden opgeslagen. Deze ideale vorm van normalisatie[3] komt echter niet altijd voor.
Dat betekent dat de accountant moet onderzoeken of de applicaties wijzigingen in semi-permanente gegevens toestaan. Indien dat zo is, moet de accountant tevens vaststellen of er een voorziening is getroffen om de oudere waarden te kunnen recapituleren (met bijvoorbeeld zogenoemde was-wordt-lijsten).
Ter toelichting: hiermee wordt invulling gegeven aan het begrip audittrail. Een audittrail is het spoor in de administratie waarbij na te gaan is:

- uit welke transacties een totaal is opgebouwd;
- hoe een transactie in een totaal is opgenomen.

IT-data zijn raadpleegbaar

Als algemeen uitgangspunt wordt aangenomen dat eenmaal vastgelegde gegevens ook raadpleegbaar zijn – waarom zou men anders gegevens opslaan? Dit raadplegen vereist altijd een voorziening in de set IT-processen. Idealiter kan de applicatie (bijvoorbeeld het ERP-pakket) waarmee de mutaties zijn ingevoerd al die gegevens herschikken, totaliseren en tonen. Zij het wel met de restrictie dat alleen gebruikers die bevoegd zijn, via deze functionaliteit de data kunnen raadplegen.
In termen van een database is het grootboek een 'view', een selectie van data, uit de corporate database. De accountant moet daarom bij de controle op de jaarrekening weten of er gegevens worden vastgelegd naast hetgeen het grootboek hem laat zien (zijn er transacties of mutaties buiten het grootboek gehouden?). In aanvulling hierop zal de accountant willen vaststellen dat records met

mutaties ook de gegevens bevatten van degene die de records heeft toegevoegd én wanneer hij die heeft toegevoegd. In beginsel dient de accountant de betreffende records ter beschikking te hebben.
Hiermee komen twee vragen naar voren. De juistheidsvraag (zijn de gepresenteerde gegevens juist, geautoriseerd en dergelijke) kan indicaties opleveren dat verantwoorde omzetten eigenlijk niet in de praktijk zijn gerealiseerd. De volledigheidsvraag is de vraag of al dan niet bewust een deel van de feitelijke omzet of kosten buiten de boeken wordt gehouden.

Autorisaties

Alleen geautoriseerde medewerkers moeten data (mutaties) kunnen toevoegen. De schil in figuur 2 moet er daarom voor zorgen dat gebruikers selectief toegang krijgen tot IT-processen en IT-data. In het proces 'inloggen' wordt aan de hand van het user-id de gebruiker geïdentificeerd en dient het password ter authenticatie.[4] Daarna verkrijgt de gebruiker binnen die schil de aan de gebruiker toegekende bevoegdheden tot het gebruik van IT-processen zodat alleen de toegekende activiteiten zoals data raadplegen, toevoegen, verwijderen en/of muteren worden uitgevoerd.
De accountant dient te onderzoeken of en in hoeverre andere gebruikers dan de geautoriseerde gebruikers dergelijke activiteiten (zoals data toevoegen) uitvoeren.
Enkele voorbeelden van toevoegingen die buiten de reguliere gebruikers om zijn doorgevoerd, zijn:

- het opnieuw opbouwen van een database na conversie naar een nieuwe editie van een ERP-pakket;
- het herstellen van een database na een onderbreking.

Dergelijke toevoegingen kunnen een forse inbreuk opleveren op het gewenste niveau van betrouwbaarheid en beschikbaarheid van informatie. Daarom zijn specifieke maatregelen vereist rond deze "changes".

Maatregelen

Deze paragraaf bevat een beknopte beschrijving van maatregelen.
Indien de accountant de interne beheersing bij de controle gebruikt, dient hij steeds te onderzoeken of aan alle uitgangspunten is voldaan. Daarom is een minimale set *general IT-controls* nodig om zowel de toegangsbeheersing, als het change management en het slechts kunnen toevoegen van data, met behulp van de applicatieprogrammatuur van de gecontroleerde organisatie, aan de corporate database te realiseren.
Omdat de interne beheersing van de IT ook grotendeels opgenomen is in die IT betekent dit ook dat tenminste vereist is dat de logische toegangsbeheersing is ingericht op zowel het niveau van general controls als dat van application controls.[5]

De accountant moet zodanig toetsen dat hij antwoord kan geven op de vraag of in de onderhanden casus niet van de uitgangspunten wordt afgeweken, en als er wel van de uitgangspunten wordt afgeweken, dat er voldoende maatregelen zijn genomen om negatieve gevolgen te voorkomen. Onder negatieve gevolgen valt bij de jaarrekeningcontrole vooral te denken aan beperkingen van de controleerbaarheid.

Voorafgaand aan de feitelijke controlewerkzaamheden moet de accountant weten hoe de IT binnen de organisatie is vormgegeven, welke IT-infrastructuur aanwezig is, welke IT-processen daar gebruik van maken, welke IT-data[6] daarbij horen en welke handmatige processen op een en ander aansluiten. Deze onderwerpen illustreren wij hierna kort met enkele voorbeelden.

General controls met betrekking tot de wijze waarop de IT binnen de organisatie is georganiseerd betreffen, globaal omschreven, maatregelen als:

- aansluiting van IT met de business (alignment) met betrekking tot strategie, management, organisatieontwerp en bedrijfsactiviteiten en business rules;
- ontwerp van bevoegdheden en verantwoordelijkheden van de IT-organisatie in relatie tot gebruikers;
- ontwerp van procedures, technische en fysieke maatregelen ter ondersteuning van de toepassing van de gedefinieerde bevoegdheden;
- monitoring[7] op naleving en signalering afwijkingen;
- change management op ontwerp en toepassingsprogrammatuur.

General controls ter bescherming van de technische IT-infrastructuur betreffen, globaal omschreven, maatregelen als:

- definiëring/ontwerp van de IT-infrastructuur, inclusief systeemprogrammering, applicaties en datacommunicatienetwerken;
- fysieke en logische toegangsbeheersing tot de (componenten[8] van de) infrastructuur;
- monitoring op naleving en signalering afwijkingen;
- change management op ontwerp en toegang.

General controls ter bescherming van de IT-processen zijn dan globaal te omschrijven met maatregelen als:

- definiëring/ontwerp van de functionele IT-processen in relatie tot de processen binnen de organisatie van de gebruikers en de architectuur van de andere IT-processen;
- ontwerp van de logische toegangsbeheersing binnen de IT-processen op basis van bijvoorbeeld *need to know* en/of *need to use*-principes;
- change management, inclusief ontwikkelorganisatie, op ontwerp en implementatie;
- monitoring van wijzigingen – eventueel met behulp van logging van die monitoringactiviteiten;
- definiëring van de IT-processen en de application controls in samenhang met de handmatige processen en controles.

General controls ter bescherming van de IT-data zijn globaal te omschrijven met maatregelen als:

- definiëring/ontwerp van de data-architectuur, met het oog op control over afwijkingen ten opzichte van het theoretisch model van een corporate database;
- logische toegangsbeheersing tot (clusters) van data op basis van bijvoorbeeld need to know en/of need to use;
- monitoring van wijzigingen van data-architectuur en logische toegangverlening;
- change management bij toevoegingen of veranderingen buiten de reguliere applicaties om.

Deze general controls richten zich dus op de definiëring, de implementatie, de monitoring en de changes. Deze controls moeten op zichzelf ook weer gedefinieerd, et cetera, worden zodat hiervoor weer waarborgen vereist zijn. Vervolgens geven deze controls weer waarborgen rond de engineering van IT-aanpassingen.
Onder engineering verstaan we een proces waarin procedures, kaders en normen waarborgen dat de wijzigingen worden ontworpen en geïmplementeerd die door het management van de organisatie waren bedoeld. De engineering bevat ook de maatregelen van informatievoorziening, monitoring en evaluatie om vast te kunnen stellen dat de engineering goed is verlopen. In bestaande situaties is het begrip re-engineering van toepassing.

Logische toegangsbeheersing

Het onderwerp logische toegangsbeheersing verdient hier nog een aantal opmerkingen. De toegang tot de infrastructuur kent twee aspecten. Toegang tot operationele data en IT-processen én toegang tot de toegangsregeling. Omdat de toegangsregeling een zeer belangrijke rol vervult, zijn waarborgen rond dit proces vereist. De bevoegdheden tot de toegang tot het toegangbeheer en het kunnen aanbrengen van veranderingen, zoals bevoegdheden van gebruikers, moet daarom ook geregeld zijn.

De grote lijn van logische toegangscontrole geldt ook hier: identificeren en authenticeren en pas daarna wordt de gevalideerde identiteit geautoriseerd tot handelingen.
Een paar voorbeelden:

- Enkel het inpluggen van een notebook in een (zowel vast als draadloos) netwerk is eigenlijk al een wijziging van de infrastructuur. Er zijn dus maatregelen zoals regels en normeringen nodig om de toegang tot een netwerk te sturen en te beheersen.
- Het zonder meer koppelen van een *local network* aan het internet via een bridge is een bijna ongebreidelde *change* van het netwerk. Door zo'n koppeling gaat het locale netwerk deel uitmaken van het openbare www-netwerk.

Ook de toegang tot IT-processen om IT-data en/of IT-processen te veranderen, vraagt om gericht change management. Bestaande IT-processen kunnen worden verwijderd en ze kunnen worden geüpdatet. Omdat dergelijke wijzigingen ingrijpende gevolgen kunnen hebben voor de interne beheersing en de bedrijfsvoering kennen dergelijke wijzigingen en updates de nodige risico's. Het kunnen verwijderen en updaten vraagt derhalve om gepaste maatregelen. In dit kader gaan we niet verder in op het 'gewone' gebruik van toegangsbeheer omdat daar geen aanvullende bijzondere maatregelen nodig zijn.

De toegang tot de IT-data, die plaatsvindt via IT-processen, dient onder meer te bewerkstelligen dat data slechts eenmaal worden vastgelegd. Zoals hiervoor is omschreven, is de norm dat de eenmaal vastgelegde data wel geraadpleegd kunnen worden, maar niet gewijzigd. Er zijn in de applicatie(s) dus voorzieningen nodig die kunnen zorgen voor het enkel toevoegen van gegevens. Een mogelijkheid tot het wel kunnen wijzigen van eenmaal vastgelegde data is te beschouwen als een bedreiging van de integriteit van de data.
Een paar voorbeelden:

- Het aanpassen van semipermanente data (ook wel: 'vaste gegevens' genoemd, bijvoorbeeld de bankrekeninggegevens van een leverancier) is het aanbrengen van wijzigingen en niet een toevoeging van gegevens. Toevoegen is de 'normale' beheerste, en dus veronderstelde wijze van organiseren.
- Ook het corrigeren van een record moet als een wijziging van een vastlegging worden beschouwd.

Het kunnen raadplegen van data is in beginsel geen bedreiging van de betrouwbaarheid, tenzij de data gevoelig is. Het hanteren van het zogenoemde need to know-uitgangspunt kan men zien als het beperken van toegang tot slechts die gegevens die bij een besluitvormingsproces nodig zijn. Vanuit een besluitvormingsproces worden de benodigde data gedefinieerd en door middel van een view ter beschikking gesteld, ongeacht de overige bevoegdheden van de betreffende identiteit.
Indien dit principe wordt toegepast biedt een beoordeling van alle toegekende need to know-elementen per functionaris een beeld van alle toegekende in de schil opgenomen IT-bevoegdheden waarbij bepaalde combinaties minder wenselijk zijn (functievermenging).

Samenvattend: de accountant moet met betrekking tot de IT van de klant de uitgangspunten, die zijn geformuleerd als een normstelling, kennen. Vervolgens dient hij te onderzoeken of die normen worden nageleefd. Als per uitgangspunt de afwijkingen worden geïnventariseerd, zijn ook de beheersingsmaatregelen die dienen om die afwijkingen het hoofd te bieden, te bepalen en op effectiviteit te beoordelen.

HET TRANSACTIEMODEL

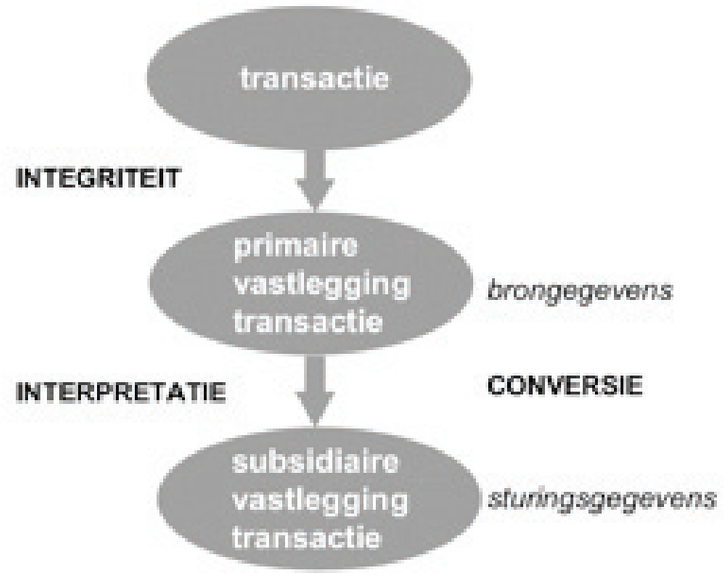
Een financiële verantwoording is opgebouwd uit data van de organisatie en is een weergave van de financiële standen op een moment en van mutaties over een periode. Deze data zijn afkomstig uit verschillende registraties die worden gevoed door gebeurtenissen of transacties *in the real world* en de daarmee samenhangende primaire vastleggingen. Veel primaire vastleggingen worden rechtstreeks gedaan in de sfeer van de IT, maar nog steeds vinden er primaire vastleggingen plaats buiten 'het systeem'. Voor de accountant is het van belang dat de primaire vastleggingen (gaan) overeenstemmen met wat zich in de werkelijkheid afspeelde. In eerste instantie is dan niet van belang of die vastleggingen op papier plaatsvinden of direct binnen de IT-omgeving.

Het transactiemodel[9] (zie figuur 3) is een model dat het ontstaan van registraties in een registratiesysteem van een organisatie visualiseert.
In figuur 3 is het model 'kaal' weergegeven. Figuur 4 geeft het transactiemodel weer in relatie tot clusters informatiesystemen.

De drie 'omgevingen' van het transactiemodel houden het volgende in:

- De eerste omgeving vertegenwoordigt de 'real world' waarin de transacties (gebeurtenissen) plaatsvinden. In deze bol bevinden zich geen gegevens.
- De tweede omgeving geeft weer dat van elk van de transacties een primaire vastlegging wordt gemaakt in de wereld van de gegevens. In deze bol bevinden zich de eerste (of primaire) vastleggingen van de transacties.
- De derde omgeving representeert de vertaling van de gegevens van de primaire vastleggingen naar de wereld van de informatie.

Dat betekent dat de gegevens van de primaire vastlegging worden geïnterpreteerd tot een set gegevens die toereikend is voor het (formele) informatiesysteem waarin ze worden opgenomen. Aan de gegevens van de primaire vastleggingen worden gegevens zoals organisatorische eenheid, medewerker die transactie verricht/invoert, periodeaanduiding en dergelijke, toegevoegd. In de papieren wereld gebeurde dat bijvoorbeeld door het plaatsen van een blokstempel en het invullen van de velden ervan op de brondocumenten (naam, kostenplaats, datum et cetera). In de elektronische wereld koppelt men usergegevens en dergelijke aan de primaire vastleggingen.



Figuur 3: Transactiemodel met drie sferen of omgevingen[10]

Het model laat zien wat men wel, en wat men niet achteraf kan onderzoeken. Zo is achteraf niet vast te stellen wat zich allemaal in de vluchtige 'real world' heeft voorgedaan, omdat niet alles doorlopend wordt geregistreerd. Achteraf is het wel mogelijk de Ist-posities van de derde omgeving, die met subsidiaire vastleggingen, te vergelijken met de primaire vastleggingen in de tweede omgeving. Daartoe moeten die primaire vastleggingen eerst tot een Soll-positie worden opgewaardeerd.

Het model maakt zichtbaar dat de 'primaire vastleggingen' worden geïnterpreteerd. Dat wil zeggen: de primair vastgelegde gegevens worden gefilterd en verrijkt met andere gegevens[11] om te voldoen aan de informatiebehoeften die tot uitdrukking zijn gebracht in de formele informatiesystemen. Deze interpretatie of vastlegging dient als basis voor de omgeving van de subsidiaire vastleggingen (derde omgeving) waartoe ook de gegevens van de jaarrekening behoren.

Zoals hiervoor gesteld, is het van belang dat de primaire vastleggingen overeenstemmen met wat zich in de werkelijkheid afspeelde. Dit maakt de overgang van 'real world' naar primaire vastlegging kritisch. Daarom dienen steeds de volgende vragen te worden gesteld, zowel voorafgaand aan de periode waarvan de verantwoording wordt gecontroleerd als gedurende de controle van de verantwoording.

- Worden wel alle gedefinieerde transacties in een bepaalde periode vastgelegd (volledigheid)?
- Geeft de projectie wel een compleet beeld? Dat wil zeggen: worden wel alle gedefinieerde relevante ▶

metadata over de transactie(s) vastgelegd (compleetheid metadata) om de informatiebehoeften te vervullen?
- Zijn de vastgelegde gegevens (velden) per weergave (record of view van een serie records) wel juist (juistheid)? 'Juist' is dan juist, gezien door de ogen van de gebruikers van de (subsidiaire) vastleggingen.

Uit bovenstaande blijkt reeds dat sturing plaats vindt door het definiëren van de te registreren transacties en gegevens.

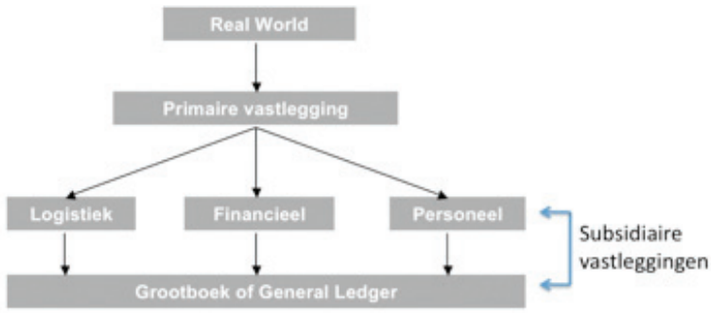
Zoals aangegeven toetsen accountants in hun onderzoek de Ist-posities (de subsidiaire gegevens) aan Soll-posities (de primaire vastleggingen). Voor de uitvoering van die toetsing achteraf, moeten de primaire vastleggingen dus voldoen aan de kwaliteit 'Soll-positie'. Om deze kwaliteit te verkrijgen, moeten die primaire vastleggingen getoetst zijn aan de 'real world'. Deze toetsing zal veelal gelijktijdig met de primaire vastlegging moeten zijn uitgevoerd.

Een opwaardering van Ist-gegevens, zoals de primaire vastleggingen, tot vastleggingen met Soll-kwaliteiten is bijvoorbeeld mogelijk door over de schouder mee te kijken van degenen die de transactie uitvoeren. De uitdaging voor primair het management en secundair de controlerend dan wel adviserend accountant is om middelen en methoden te vinden die een equivalent zijn van het 'over de schouder meekijken'. Maatregelen kunnen zijn: het organiseren van zogenaamde 'tegengestelde belangen' (bijvoorbeeld kwijting bij afgeven en ontvangen van goederen), het laten bevestigen van gebeurtenissen door een relatieve buitenstaander (zoals aftekenen urenbriefje bij uitzendkracht), de toepassing van het twee paar ogen principe (beroep op verantwoordelijkheid voor registratie) en dergelijke.[12]

Het model maakt ook duidelijk dat er omstandigheden kunnen zijn die een toetsingsonderzoek (vergelijking van Ist- met Soll-posities) niet meer mogelijk maken zoals bij niet geregistreerde gebeurtenissen en bij verloren gegane primaire vastleggingen zonder herstelmogelijkheid zoals bijvoorbeeld bij bepaalde vormen van dienstverlening.

Het model laat zien dat bij compliance-tests de subsidiaire vastleggingen (Ist) worden vergeleken met primaire vastleggingen (a priori Ist-posities, mogelijk bruikbaar als 'Soll') en eigenlijk niet de werking van het juist en volledig registreren van de 'real-world' wordt getoetst. Cruciaal bij het verrichten van compliance-tests is de vraag of de primaire vastleggingen al door middel van toetsing zijn opgewaardeerd van Ist-positie tot Soll-positie. Ofwel de vraag of middelen en methoden als equivalent van 'over de schouder meekijken' zijn geïmplementeerd en effectief gebleken.

In figuur 4 is het transactiemodel ingevuld met de soorten systemen die in de sfeer van de subsidiaire vastleggingen worden aangetroffen. Voor de eenvoud zijn de schattingssystemen[13] achterwege gelaten.



Figuur 4: Transactiemodel in relatie tot clusters informatiesystemen

De primaire vastleggingen hebben verschillende kenmerken die leiden tot registratie in verschillende clusters informatiesystemen. Het hangt van de casuïstiek af of er sprake is van dergelijke (losse) clusters of dat er sprake is van een ERP-systeem[14] met geïntegreerde functionele modules. Zoals eerder aangegeven, ontstaan bij clusters (ook wel eilandautomatisering genoemd) mogelijk synchronisatieproblemen en allerlei interfaces die juistheidrisico's met zich brengen. Het grootboek kan dan wel de rol van het 'netwerk van controletotalen' vervullen. Bij een ERP-systeem is in dat netwerk in potentie voorzien en zou het grootboek slechts een view op de (relationele) database moeten betreffen. Het grootboek heeft in dat geval niet per se een controletechnische betekenis, maar is vooral van belang voor de presentatie van de geaggregeerde gegevens over het bedrijfsgebeuren.

Voor de financiële controle is met name de blijvende juistheid van de eenmaal vastgelegde data van belang. Hiervoor is het uitgangspunt behandeld dat data omtrent transacties alleen worden toegevoegd en raadpleegbaar zijn. Afwijkingen van dit uitgangspunt tasten de controleerbaarheid aan. Dit is bijvoorbeeld het geval bij de toepassing van Excel sheets, waarin gegevens wel worden verwijderd en vervangen door nieuwe waardoor achteraf deze mutaties niet meer herleidbaar zijn naar de oorspronkelijke boekingen. Voor de financiële controle zijn dus maatregelen vereist die de verschillende versies van data 'conserveren'.

Het transactiemodel is op deze manier een referentiekader voor het beoordelen van de onvervangbare interne beheersing van de organisatie waarin zowel handmatige als geautomatiseerde elementen te onderkennen zijn. Hiermee komt het aspect IT in beeld.

VOORUITBLIK OP DEEL 2

Deel 2 van het artikel zal ingaan op de zogenoemde 'doelstellingen informatietechnologie' in relatie tot het transactiemodel. De auteurs lichten de historie en de achtergrond van 'de drie doelstellingen' toe. Daarmee komt het praktisch kader[15] van de doelstellingen aan bod. Het tweede deel sluit af met een korte samenvatting van beide delen. ■

Noten

1 Wij hanteren het begrip 'risico' hier als de kans op een ongewenst effect.

2 Bij eilandautomatisering is er sprake van een veelheid aan applicatieprogramma's. Zo kunnen personeelsinformatiesysteem, salarisberekening, grootboek, logistiek informatiesysteem en financieel informatiesysteem allemaal afzonderlijke applicaties zijn. Bij die applicaties is er sprake van data-overlap. Dat fenomeen pleegt te worden ondervangen door middel van interfaces. Interfaces vereisen extra sturings- en beheersingsmaatregelen.

3 Normaliseren is een ontwerpproces. Daarmee probeert men zoveel de gegevens slechts een keer vast te leggen. Aan databasenormalisatie is de naam Codd verbonden. De hier beschreven vorm zorgt ervoor dat een query op de database op ieder moment kan worden uitgevoerd en steeds tot dezelfde uitkomst leidt. Zo verschijnt op een veel later gemaakte afleverbon niet het huidige afleveradres, maar het adres op het moment van het creëren van de aflevergegevens.

4 Met authenticatie wordt beoogd met bepaalde zekerheid de identiteit van een gebruiker (persoon of andere computer) vast te stellen. Toetsing vindt plaats aan de hand van echtheidskenmerken die op een andere wijze binnen de toegangsregeling bekend zijn geworden. Dit kunnen zijn: iets dat men kan weten zoals een wachtwoord, pincode, een geheime zin, of een antwoord op een privévraag; iets dat men (uniek) kan bezitten zoals chipkaart, TAN-code bij banken; iets dat de gebruiker (uniek) maakt (eigenschap) zoals een (eerder aan de persoon gekoppelde) iris of vingerafdruk.

5 In het toepassingsprogramma moet tenminste worden uitgevraagd of de betreffende persoon al is geïdentificeerd en die identiteit al met goed gevolg is geauthenticeerd. Verder moet tenminste vastliggen welke activiteiten deze identiteit mag ondernemen. Die activiteiten kunnen zijn IT-deelprocessen en data die met die deelprocessen verband houden mogen dan door die identiteit worden toegevoegd.

6 Daarbij hoort de definitie van de data – dat wil zeggen de feitelijke data architectuur.

7 Met de term 'monitoring' wordt hier een intensieve vorm van toezicht bedoeld, die nadert tot continu en direct toezicht, althans daarmee inhoudelijk in redelijke mate vergelijkbaar is.

8 Zoals terminals, computers, datacommunicatielijnen, servers en dergelijke, al dan niet met inbegrip van *bring your own devices* (Byod), mobiele telefoons en dergelijke.

9 Een van de auteurs heeft dit model toegepast in een groot aantal interne publicaties van de Belastingdienst. Een paar ervan zijn: 'Controleren met Nieuwe Grenzen' en 'Optimalisatie van Controlebeslissingen'. Deze twee gaan over het vormen van controlemodellen met behulp van theoretische modellen, waaronder statistische. Het transactiemodel is beknopt terug te vinden in [KLO002].

10 De term 'sturingsgegevens' in de afbeelding moet ruim worden uitgelegd zodat ook gegevens ten behoeve van het informeren, van de bijsturing en van het afleggen van verantwoording eronder worden begrepen.

11 Waaronder een audit-trail, de actoren die registeren, accorderen, en dergelijke.

12 Ter ondersteuning van de toetsing van subsidiaire gegevens worden ook activiteiten verricht ter vaststelling van de 'real world', bijvoorbeeld door inventarisatie en waarneming ter plaatse.

13 Balansposten zoals waardering van activa en voorzieningen et cetera zijn immers schattingen.

14 Het (theoretisch) gegevensmodel van een ERP-systeem gaat ervan uit dat een grootboek slechts een presentatie is van gegevens die al vastliggen in de (corporate) database. Het grootboek is als het feitelijke en het theoretische gegevensmodel elkaar dicht naderen, dus geen 'netwerk van controletotalen' meer, maar een zogenoemde 'view' op de vastgelegde data.

15 Praktisch kader' mag ook gelezen worden als *best practice*-kader.

Literatuur

[KLO002] Kloosterman, H.H.W, A.J. Lok en P.C. Waas, (2002). Elektronisch factureren, belastingcontrole en daaraan gerelateerde IT-audit, *Handboek EDP- auditing*, hoofdstuk 9610, Kluwer, Deventer.

[KOUT13] Kouters, I. en A.J. van der Meer (2013). Audit Integration moet gaan 'vliegen', *Accountant*, maart 2013, pp 25-27.

Hein (H.H.W.) Kloosterman RE RA is betrokken bij de accountantsopleiding van de Business Universiteit Nyenrode en de Erasmus Universiteit (ESAA), en bij de IT-auditopleiding van de VU. Verder is hij lid van de redactieraad van het Handboek EDP-auditing en van de Stuurgroep Statistical Audit en werkt hij als zelfstandig adviseur op het gebied van IT-audit en Statistical Audit.

Ruud (R.) Snoeker RA is sinds 2001 zelfstandig gevestigd als interim manager en consultant op het gebied van governance, control en risicomanagement. Daarvoor heeft Ruud verschillende managementfuncties vervuld bij financiële instellingen. Na een aantal jaren van docentschap, sinds 2007 director program internal control accountancy aan de accountantsopleiding van de Erasmus Universiteit (ESAA).