Formulering oordeel van een IT-auditor

Drs. R.J.M. van Langen RA, T. Shioda en mw. drs. M.J.A. Koedijk RA

De aard en reikwijdte van de IT-auditwerkzaamheden in het algemeen zijn zeer divers. Wel zal een IT-audit altijd uitmonden in ten minste één oordeel met betrekking tot de bevindingen. Tot op heden zijn door NOREA geen richtlijnen opgesteld inzake de wijze waarop dit oordeel moet worden geformuleerd. Eenduidigheid in formuleringen is, naar onze mening, binnen de beroepsgroep wenselijk. Hierdoor kunnen uitingen van IT-auditors door de gebruiker, veelal de opdrachtgever, beter worden vergeleken en begrepen. In dit artikel wordt ingegaan op de elementen die in een oordeel moeten worden benoemd en wordt een voorbeeld van een oordeelsformulering gegeven.

Inleiding

Binnen de accountancyopleiding wordt bij het vak controleleer uitgebreid stilgestaan bij het verklaringenstelsel. De werkzaamheden van een accountant bestaan grotendeels uit het geven van een oordeel omtrent de getrouwheid van één soort verantwoording, namelijk de jaarrekening. Binnen IT-auditing is geen verklaringenstelsel aanwezig, het object, de aard en de reikwijdte van een IT-audit zijn veelal zeer divers van aard en een specifieke verantwoording van de opdrachtgever ontbreekt vaak.

Om te komen tot een standaardformulering van een IT-auditor heeft Taroh Shioda in het kader van zijn afstudeeropdracht voor de Hanzehogeschool eind 2000/begin 2001 een onderzoek uitgevoerd. De uitkomsten hiervan zijn in dit artikel opgenomen. Om niet te verzanden in de hoeveelheid soorten opdrachten en de daarmee samenhangende uitingen van IT-auditors, is zijn onderzoek beperkt tot formuleringen van oordelen die bij systeem- of procesbeoordelingen worden afgegeven. Voor het beoordelen van processen kan gebruik worden gemaakt van de Business Process Analysis (BPA)-methodiek (zie ook [Koed99]). De BPA-opdrachten zijn in behoorlijke mate gestandaardiseerd, waardoor ook uitingen omtrent de uitkomsten van dit soort opdrachten mogelijkerwijs kunnen worden gestandaardiseerd. Daarnaast wordt de BPA-methodiek vaak gebruikt om in het kader van de jaarrekeningcontrole de daartoe aangewezen processen te beoordelen. Ook voor een accountant is eenduidigheid van de uitingen van een IT-auditor, naar onze mening, wenselijk, zoals zal worden toegelicht in de volgende paragraaf.

Allereerst wordt in dit artikel nog nader ingegaan op het nut van standaardformuleringen van oordelen, vervolgens wordt ingegaan op relevante literatuur en regelgeving. Tot slot wordt een voorbeeld van een standaardformulering van een IT-auditor gegeven en worden specifieke aandachtspunten hierin behandeld.

Het nut van standaardformuleringen van oordelen

Tot op heden worden nog geen standaardformuleringen voor IT-audits gebruikt. Wij onderkennen hiervoor drie hoofdredenen, waarop kort zal worden ingegaan:

* klantspecifieke redenen;
* geen richtlijnen van de NOREA;
* jong verleden van IT-audits.

Bij de opdrachtformulering zullen de scope en het object van een IT-onderzoek worden bepaald door wensen van de klant. De IT-auditor zal na het IT-onderzoek een rapport opstellen dat op deze klantspecifieke situatie is afgestemd. Dit is een reden dat oordelen van een IT-auditor qua formulering en indeling onderling van elkaar kunnen verschillen.

Een andere reden waarom momenteel de standaard ontbreekt, is dat de beroepsorganisatie van IT-auditors, NOREA, wel richtlijnen in het kader van de attestfunctie heeft opgesteld voor bijvoorbeeld ‘Rapportage’, maar dat in deze richtlijn geen standaardformuleringen van oordelen van onderzoeken die worden uitgevoerd door IT-auditors zijn toegevoegd. Dit in tegenstelling tot het Koninklijk NIVRA, dat wel een verklaringenstelsel heeft voorgeschreven. Echter, bij een jaarrekeningcontrole is het object één soort verantwoording die wordt gecontroleerd ten behoeve van het maatschappelijk verkeer, bij IT-auditing kan het onderzoeksobject divers van aard zijn.

IT-auditing is ontstaan met de opkomst van geautomatiseerde omgevingen. Het accountantsberoep bestaat daarentegen al ruim een eeuw. Daarnaast zijn geautomatiseerde omgevingen en het vakgebied IT-auditing nog sterk aan verandering onderhevig. Standaardisering met betrekking tot uitkomsten van onderzoeken bij IT-auditing staat dus nog in de kinderschoenen.

Betrokkenen bij oordelen van IT-auditors

De uitkomsten van IT-audits worden door diverse betrokkenen gebruikt. Om te komen tot een standaardoordeel is het zinvol om de betrokkenen te onderkennen. In tabel 1 hebben wij een overzicht van betrokkenen bij een IT-audit opgenomen.

Vanuit het perspectief van iedere betrokkene wordt hieronder kort aangegeven waarom standaardteksten voor oordelen nuttig kunnen zijn (zie ook tabel 2).

De klant
In de meeste gevallen is de klant zelf de opdrachtgever van een IT-audit. Voordat een IT-audit van start gaat, is de opdrachtformulering van belang. De opdrachtformulering omvat onder andere het object en de te beoordelen kwaliteitsaspecten, reikwijdte (waaronder opzet, bestaan en/of werking) en de te gebruiken normstelling en standaarden ([NOREA99]). Doordat al deze factoren een rol spelen bij de uitvoering van een IT-audit, kan het uiteindelijke oordeel, nog afgezien van de strekking, qua formulering sterk variëren. Het risico bestaat dat gelijksoortige opdrachten voor één opdrachtgever leiden tot verschillende formuleringen van oordelen. De schriftelijke rapportage daarover dient zodanig te zijn dat interpretatieverschillen worden vermeden.

De IT-auditor
Het is voor de IT-auditor van belang dat er geen verwachtingskloof ontstaat tussen hem en degenen die gebruikmaken van het oordeel. Zoals hierboven beschreven zijn er veel aspecten die bij de opdrachtformulering moeten worden bepaald. Uit praktisch oogpunt is het nuttig dat standaardformuleringen beschikbaar zijn om er zodoende zeker van te zijn dat alle verplichte elementen zijn opgenomen die een oordeel moet bevatten.

De accountant
De accountant kan gebruikmaken van de bevindingen van de IT-auditor voor de controle van een jaarrekening. De IT-auditor zal de accountant ondersteunen in het aanleveren van controlebewijs over de opzet, het bestaan en de werking van de beheersingsmaatregelen in de automatiseringsorganisatie en geautomatiseerde systemen ([Jonk00]). Ook hierbij is het van belang dat de oordelen van IT-audits eenduidig van aard zijn, zodat interpretatieverschillen worden vermeden.

Overige doelgroepen
Alhoewel een nauwe relatie bestaat tussen doelgroep en opdrachtgever, hoeft het niet altijd zo te zijn dat deze twee dezelfde zijn. Toezichthoudende instanties zoals DNB, STE, Verzekeringskamer en het Ctsv kunnen om hun toezichthoudende taken goed te kunnen uitoefenen om de uitkomsten van specifieke IT-audits vragen. Daarnaast kan zeker bij grote ondernemingen een verschil tussen opdrachtgever en verantwoordelijke partij worden onderkend. Een directie van een onderneming kan specifiek vragen om een audit van een object waar een afdeling verantwoordelijk voor is.

Als de doelgroep niet tevens opdrachtgever is, is meestal sprake van een 'third party'-onderzoek ([NIVRA89]). In die gevallen is het van essentieel belang dat eenduidigheid bestaat in de strekking van de oordelen, aangezien de doelgroep de opdracht niet formuleert. In het buitenland heeft men voor 'third party'-onderzoeken al voorbeelden ontwikkeld van standaardmededelingen. In de Verenigde Staten staan in SAS 70 (Statements on Auditing Standards) voorbeelden van standaardmededelingen van IT-auditors bij 'third party'-onderzoeken, in het bijzonder bij serviceorganisaties ([AICPA97]).

* De klant	In de meeste gevallen is deze de opdrachtgever van een IT-audit.
* De IT-auditor	Deze persoon geeft het oordeel af.
* De accountant	Hij/zij kan vaak een IT-auditor inschakelen voor een IT-onderzoek in het kader van een jaarrekeningcontrole.
* Overige doelgroepen	Hiermee worden bijvoorbeeld groepen bedoeld binnen het maatschappelijk verkeer die mogelijk gebruikmaken van het IT-auditrapport.

Tabel 1. Overzicht betrokkenen bij een IT-audit.

* Eenduidigheid
* Ondubbelzinnigheid
* Vaktechnisch compleet
* Voorkomen van interpretatieverschillen
* Onderlinge vergelijkbaarheid

Tabel 2. Het nut van standaardformuleringen van oordelen.

Elementen en gradaties van een oordeel van een IT-auditor

Een oordeel dat wordt afgegeven door een IT-auditor (RE) zal moeten voldoen aan de eisen die NOREA heeft gesteld in de richtlijnen in het kader van de attestfunctie, waaronder de richtlijn 'Rapportage'. Hierin is opgenomen dat een rapportage een samenhangend en aannemelijk geheel moet vormen van ten minste de volgende componenten:
* de met de opdrachtgever overeengekomen en door de RE aanvaarde opdracht of een expliciete verwijzing daarnaar;
* een beschrijving van de wijze van uitvoering van de opdracht, waaronder een beschrijving van de gehanteerde aanpak, een en ander voorzover relevant voor de uitingen;
* ten minste één oordeel met betrekking tot de bevindingen en, in voorkomende gevallen, ook de andere uitingen dan wel een expliciete verwijzing daarnaar;
* de periode van onderzoek waarbinnen de waarnemingen die de grondslag hebben gevormd voor de uitingen, tot stand zijn gekomen;
* de onweerlegbare vermelding welke RE verantwoordelijk is voor de uitingen.

Daarnaast zijn ook andere literatuurbronnen beschikbaar waarin formuleringen van oordelen zijn beschreven, zoals NIVRA-geschrift 53. Hieronder worden eerst de (verplichte) elementen behandeld die tot uitdrukking behoren te komen in een oordeel en vervolgens wordt kort stilgestaan bij de mogelijke gradaties of strekkingen van een oordeel van een IT-auditor.

Elementen van een oordeel

De elementen zijn onderverdeeld in drie gebieden naar analogie van accountantsverklaringen. Deze indeling zal herkenbaar zijn bij veel IT-auditors, met name bij hen die ook tot accountant zijn opgeleid. Door deze herkenbaarheid zou wellicht de toepasbaarheid van de formuleringen kunnen vergroten. De drie aandachtsgebieden zijn:
* doelstelling en object;
* werkzaamheden;
* oordeel.

- Datum opdrachtbevestiging
- Objectomschrijving
- Reikwijdte
- Kwaliteitsaspecten
- Definiëring van de kwaliteitsaspecten
- Verantwoordelijkheden

Tabel 3. Elementen van beschrijving doelstelling en object.

Doelstelling en object
De inleiding van het oordeel van een IT-auditor bestaat uit een omschrijving van doelstelling en object. In tabel 3 zijn de onderdelen van doelstelling en object opgenomen die hieronder kort worden toegelicht

Datum opdrachtbevestiging
Eén van de componenten in de rapportage of het oordeel dient een duidelijke verwijzing naar de opdracht te zijn, conform de eisen van NOREA. Door het opnemen van de datum van de opdrachtbevestiging kunnen misverstanden worden voorkomen.

Objectomschrijving
In het oordeel dient de beschrijving van het onderzoeksobject te worden opgenomen. Immers, indien de afbakening van het object zich tijdens het onderzoek wijzigt, dient het onderzoeksobject opnieuw te worden beschreven en kan niet slechts worden volstaan met de verwijzing naar de opdracht ([Praa96]). Soms is het onderzoeksobject een verantwoording, maar vaak ontbreekt deze bij een IT-audit. In hoeverre het rapport van de IT-auditor (met normen en beschrijving van bevindingen) in een dergelijke situatie als een verantwoording kan worden beschouwd, wordt niet verder in dit artikel uitgewerkt. Het onderzoeksobject omvat maatregelen binnen een bepaald proces (of systeem) ter waarborging van één of enkele kwaliteitsaspecten.

Reikwijdte
Onder reikwijdte van het onderzoek wordt in richtlijn 'Opdrachtformulering en -aanvaarding' ([NOREA99]) mede verstaan of de opzet, het bestaan en/of de werking van het object van onderzoek worden beoordeeld. Onder de opzet wordt verstaan de formele opzet van het onderzoeksobject, zoals vastgelegd in organisatieschema's, procedurebeschrijvingen en handboeken. Bij bestaan vindt waarneming van de geïmplementeerde beheersingsmaatregelen in het onderzoeksobject plaats en bij werking stelt de auditor het functioneren van de beheersingsmaatregelen over een bepaalde periode vast.

Kwaliteitsaspecten en definiëring hiervan
In de opdrachtformulering worden de te beoordelen kwaliteitsaspecten opgenomen ([NOREA99]). De kwaliteitsaspecten worden als volgt gedefinieerd: 'de invalshoeken of eigenschappen waarover met betrekking tot een object een oordeel wordt uitgesproken'. De kwaliteitsaspecten zoals betrouwbaarheid en continuïteit zijn derhalve een onlosmakelijk onderdeel van de beschrijving van het doel van de IT-auditopdracht.

- Inhoud
- Uitsluitingen
- Onderzoeksperiode
- Informatie

Tabel 4. Elementen van beschrijving werkzaamheden.

Bij objectomschrijving is reeds benoemd dat het onderzoeksobject maatregelen omvat. Dat wil zeggen dat het onderzoeksobject niet is 'de betrouwbaarheid van een proces', maar 'de maatregelen die de betrouwbaarheid van het proces moeten waarborgen'.
De te onderscheiden kwaliteitsaspecten en hun definities zijn vooralsnog niet eenduidig gedefinieerd. In ieder boek over IT-auditing zijn verschillende definities en indelingen van kwaliteitsaspecten te vinden. Om begripsverwarring bij de gebruiker van het oordeel te voorkomen is het noodzakelijk de definiëring van de kwaliteitsaspecten in het oordeel op te nemen.

Verantwoordelijkheden
Met betrekking tot de verantwoordelijkheden in de rapportage is, met uitzondering van de ondertekening, niets binnen de NOREA-richtlijnen vastgelegd. Meestal vinden IT-audits ook plaats op verzoek van de opdrachtgever waarbij tussen opdrachtgever en opdrachtnemer onderling de verantwoordelijkheden worden vastgesteld. Indien uitingen worden openbaar gemaakt is het wenselijk, naar analogie van accountantsverklaringen, om de verantwoordelijkheden van opdrachtgever en opdrachtnemer expliciet te benoemen, zodat een derde beter inzicht krijgt in het oordeel dat wordt afgegeven. De opdrachtgever is verantwoordelijk voor het treffen van de vereiste maatregelen om te voldoen aan bepaalde kwaliteitsaspecten, de opdrachtnemer voor het afgeven van een oordeel hieromtrent.

Werkzaamheden
Na de beschrijving van doelstelling en object volgt een beschrijving van de werkzaamheden. Door deze te beschrijven kan het onderzoeksobject volledig worden afgebakend ([Praa96]). In tabel 4 zijn de onderdelen van werkzaamheden opgenomen die hieronder kort worden toegelicht.

De werkzaamheden van een IT-auditor bestaan uit het beoordelen van de getroffen beheersingsmaatregelen. In het kader van de inhoud van de werkzaamheden is een omschrijving welke beheersingsmaatregelen zijn beoordeeld (bijvoorbeeld fysieke en/of organisatorische maatregelen, maatregelen in de programmatuur en/of maatregelen in de gebruikersorganisatie) wenselijk.

Volgens de *BPA Methodology Guide* maken algemene computercontroles geen onderdeel uit van een BPA-onderzoek. Deze uitsluiting behoort in het oordeel te worden omschreven, zodat de lezer duidelijkheid verkrijgt omtrent wat wel of niet is onderzocht. Indien de werking van maatregelen is uitgesloten (reikwijdte) verdient het aanbeveling om dit expliciet te vermelden, omdat dan extra duidelijkheid wordt verschaft over het feit dat het functioneren van de beheersingsmaatregelen over een bepaalde periode niet is onderzocht.

De periode van onderzoek waarbinnen de waarnemingen tot stand zijn gekomen, dient op basis van de NOREA-richtlijnen te worden opgenomen. Daarnaast kan men de periode waarover de uiting wordt gedaan, beschrijven. Bij IT-audits zijn vaak de maatregelen van een proces het object van onderzoek en ontbreekt een verantwoording over een bepaalde periode. Het oordeel kan derhalve betrekking hebben op een momentopname

(ten tijde van ons onderzoek zijn geen tekortkomingen geconstateerd) of op een bepaalde periode (gedurende het jaar 2000 zijn voldoende maatregelen in opzet getroffen om de betrouwbaarheid te waarborgen). Indien de reikwijdte ook de werking betreft, is het noodzakelijk om in het oordeel de periode te vermelden gedurende welke het onderzoek is verricht, want dan kan geen sprake zijn van een momentopname.

Het verkrijgen van informatie vormt de basis om een onderzoek uit te voeren. Een beschrijving van de wijze van uitvoering van de opdracht (inclusief een beschrijving van de gehanteerde aanpak) dient te worden opgenomen in de rapportage. Bij IT-audits kan men denken aan het houden van interviews, het bestuderen van documentatie (zoals procedurebeschrijvingen), etc.

De diepgang (of mate van zekerheid) en ook de weging van bevindingen die leiden tot het uiteindelijke oordeel, is nog niet aan bod gekomen. De BPA-methodiek is erop gericht om met een redelijke mate van zekerheid een oordeel af te geven. Bij andersoortige opdrachten kan de mate van gedetailleerdheid waarmee men het onderzoeksobject en de onderdelen daarvan wil beschouwen, verschillen. Dit heeft dus ook betrekking op de mate van zekerheid die wordt betracht bij het afgeven van een oordeel. (Vergelijk met accountantsverklaring, beoordelingsverklaring en samenstelverklaring.) Binnen het vakgebied van IT-auditing is echter nog geen breed gedragen indeling in gradaties van zekerheid beschreven. In het kader van dit artikel is dit dan ook niet verder uitgewerkt.

Oordeel

Tot slot komt de oordeelsparagraaf zelf aan de orde. Hierin wordt ondubbelzinnig het oordeel geformuleerd. Het oordeel moet aansluiten op de doelstelling van de opdracht. Dit wordt gerealiseerd door een terugkoppeling bij het oordeel naar het kwaliteitsaspect, het object en de diepgang. Tevens dient een verwijzing naar de kwaliteitseisen (toetsingsnormen) en eventueel naar de bevindingen te worden opgenomen.

Een verwijzing naar een normenkader behoort altijd te zijn opgenomen in het oordeel ([NOREA99]). Een oordeel bestaat immers uit een vergelijking tussen het te beoordelen object en een norm. De bijlage van de rapportage zal dan ook een beschrijving van de eisen moeten bevatten.

Indien de IT-auditor het wenselijk acht, is het mogelijk een toelichtende paragraaf op te nemen. Is het oordeel niet sec goedkeurend (dus afkeurend of met beperking), dan dienen de bevindingen die hebben geleid tot dit oordeel te worden opgenomen direct na de oordeelsparagraaf ([NIVRA89]).

Mogelijke gradaties of strekkingen van een oordeel van een IT-auditor

De volgende gradaties of strekkingen van een oordeel van een IT-auditor kunnen worden onderscheiden:

* *Goedkeurend.* Dat wil zeggen dat het onderzoeksobject in voldoende mate beantwoordt aan de gestelde criteria.
* *Goedkeurend met beperking.* Dat wil zeggen dat in voldoende mate kan worden vastgesteld dat het onderzoeksobject beantwoordt aan de gestelde criteria met uitzondering van enkele aspecten. Er is dan sprake van een materiële tekortkoming en/of materiële onderzoeksonzekerheid. Het totaalbeeld is echter voldoende, want anders zal een afkeurend of onthoudend oordeel moeten worden gegeven.
* *Onthoudend.* In dat geval kan niet tot een totaaloordeel worden gekomen met betrekking tot de gestelde criteria voor het onderzoeksobject. De oordeelonthouding behoeft de waarde van het onderzoek en het rapport niet teniet te doen. Niettemin kan het zeer zinvol zijn te komen tot een rapportage over de mate waarin op onderdelen wel wordt voldaan aan de gestelde criteria.
* *Afkeurend.* Dat wil zeggen dat het onderzoeksobject niet aan de gestelde criteria voldoet (wezenlijke tekortkoming). Het afgeven van een dergelijk oordeel aan andere doelgroepen dan de opdrachtgever zelf kan verstrekkende consequenties hebben.

In NIVRA-geschrift 53 is vermeld dat een oordeel met beperking niet wordt gegeven. De motivatie daarachter is dat het advies luidt geconstateerde tekortkomingen op te heffen, hetgeen na aanpassing kan leiden tot een goedkeurend oordeel. De praktijk leert echter dat niet altijd het advies (tijdig) opgevolgd kan worden. Een oordeel met beperking is dan wel zinvol om toch tot een juist oordeel te komen. De grens tussen een goedkeurend oordeel met beperking en een afkeurend oordeel zal door vakkundige oordeelsvorming moeten worden bepaald. In dit artikel wordt hier verder niet op ingegaan.

De grens tussen een goedkeurend oordeel met beperking en een afkeurend oordeel zal door vakkundige oordeelsvorming moeten worden bepaald.

Afhankelijk van de gekozen kwaliteitscriteria en het onderzoeksobject is een oordeelonthouding mogelijk. Echter, bij een onderzoek naar de betrouwbaarheid van een object zal dit soort oordeel niet vanzelfsprekend zijn. Betrouwbaarheid omvat naast vertrouwelijkheid en integriteit ook het aspect controleerbaarheid. Indien niet tot een totaaloordeel met betrekking tot de gestelde criteria kan worden gekomen (oordeelonthouding), kan ook worden gesteld dat het onderzoeksobject niet controleerbaar is. Aan het kwaliteitsaspect betrouwbaarheid wordt dan niet voldaan.

Een standaardformulering van een oordeel van een IT-auditor

Op basis van een onderzoek naar de gehanteerde formuleringen in de praktijk inzake BPA-onderzoeken en de literatuurstudie zijn uiteindelijk de standaardoordelen geformuleerd. Deze zijn afgestemd met diverse IT-auditors die BPA-opdrachten uitvoeren. De onderstreepte teksten zijn ter illustratie en zijn uitsluitend ter verbetering van de leesbaarheid toegevoegd.

De uitsluiting van de general IT controls is als voorbeeld toegevoegd. Onder welke randvoorwaarden men wel een oordeel kan geven over een proces zonder de general IT controls hierin te betrekken, wordt in dit artikel niet verder uitgewerkt. Daarnaast is in het voorbeeld ervan uitgegaan dat de werking van de maatregelen niet behoort tot de doelstelling van de opdracht.

Formulering goedkeurend oordeel

Doelstelling en object

Ingevolge uw opdracht, zoals bevestigd d.d. *2 januari 2001*, heeft *IT-auditor* een onderzoek uitgevoerd naar *de in opzet en bestaan* getroffen beheersingsmaatregelen ter waarborging van *de betrouwbaarheid* van *het inkoopproces inclusief het ondersteunende informatiesysteem INKSYS en de interfaces naar het financiële systeem FINSYS*.

Onder *betrouwbaarheid* is in dit kader begrepen de *integriteit (juistheid, volledigheid en tijdigheid), exclusiviteit (autorisaties) en controleerbaarheid*.

Het *inkoopproces* inclusief het ondersteunende *INKSYS* is ingericht onder verantwoordelijkheid van de leiding van de *huishouding*. Het is onze verantwoordelijkheid een oordeel inzake het *inkoopproces* inclusief het ondersteunende *INKSYS* te verstrekken.

Werkzaamheden

Het onderzoek heeft de beheersingsmaatregelen in en rondom systeem *INKSYS* met betrekking tot het *inkoopproces* omvat. Maatregelen in *INKSYS* zijn bijvoorbeeld geprogrammeerde controles, overzichten, totaaltellingen en signaleringslijsten. Maatregelen rondom *INKSYS* zijn door gebruikers uitgevoerde handmatige controles.
De beoordeling van de opzet van de algemene computercontroles (general IT controls) is geen onderdeel van het onderzoek geweest. Tevens merken wij op dat de beoordeling van de werking van de beheersingsmaatregelen over een bepaalde periode geen onderdeel van het onderzoek is geweest.

Het onderzoek is uitgevoerd in de periode *januari tot en met februari 2001* en is gebaseerd op *kennisname van documentatie en het houden van interviews*. Een overzicht hiervan is opgenomen in *bijlage 2*.

Oordeel

Op grond van ons onderzoek zijn wij van oordeel dat het stelsel van getroffen beheersingsmaatregelen ter waarborging van *de betrouwbaarheid* van het *inkoopproces* inclusief het ondersteunende *INKSYS* in *opzet en bestaan* voldoet aan de gestelde normen zoals beschreven in *bijlage 1*.

Formulering oordeel met beperking

Bij een oordeel met beperking verandert alleen de oordeelsparagraaf en worden de bevindingen die leiden tot dit oordeel toegevoegd. De tekst van de oordeelsparagraaf ziet er dan als volgt uit:

Op grond van ons onderzoek zijn wij van oordeel dat het stelsel van getroffen beheersingsmaatregelen met betrekking tot [kwaliteitsaspecten] van [proces X] inclusief het ondersteunende [informatiesysteem Y] in [reikwijdte] voldoet aan de gestelde normen zoals beschreven in [bijlage 1] met uitzondering van [...]. Hierna treft u de bevindingen aan die tot dit oordeel hebben geleid.

Bevindingen
[beschrijving van slechts de bevindingen die van invloed zijn op de strekking van het oordeel]

Formulering afkeurend oordeel

Bij een afkeurend oordeel verandert ook alleen de oordeelsparagraaf en worden de bevindingen die leiden tot dit oordeel toegevoegd. De tekst van de oordeelsparagraaf ziet er dan als volgt uit:

Op grond van ons onderzoek zijn wij van oordeel dat het stelsel van getroffen beheersingsmaatregelen met betrekking tot [kwaliteitsaspecten] van [proces X] inclusief het ondersteunende [informatiesysteem Y] in [reikwijdte] niet voldoet aan de gestelde normen zoals beschreven in [bijlage 1]. Hierna treft u de bevindingen aan die tot dit oordeel hebben geleid.

Bevindingen
[beschrijving van slechts de bevindingen die van invloed zijn op de strekking van het oordeel]

Tot slot

De formuleringen zijn bedoeld om op te nemen in een rapport en niet als zelfstandige uiting; wil men ze toch als zodanig hanteren, dan zullen onder andere ook opschrift, datering en adressering aan bod moeten komen.

We zijn ons ervan bewust dat dit artikel een eerste aanzet is waarbij de bruikbaarheid voor de formuleringen voor andersoortige opdrachten nog niet is getoetst. We hopen wel met dit artikel een goede aanzet te hebben gegeven om te komen tot meer standaardisatie van oordelen van IT-auditors.

Literatuur

[AICPA97]
American Institute of Certified Public Accountants, The AICPA Professional Standards AU Section 324, *Reports on the Processing of Transactions by Service Organizations* (SAS 70), AICPA, 1997, p. 395-413.

[NIVRA89]
Koninklijk Nederlands Instituut Van Registeraccountants, NIVRA-geschrift 53 *Automatisering en controle Deel VII. Kwaliteitsoordelen over informatievoorziening*, Kluwer Bedrijfswetenschappen, Deventer 1989.

[IFAC00]
International Federation of Accountants, *International Standard on Auditing 100, Assurance Engagements*, juni 2000.

[Jonk00]
R.A. Jonker RA en drs. R.J.M. van Langen RA, *Samenwerking financial auditor en EDP-auditor*, Compact 2000/2.

[NOREA99]
Nederlandse Orde van Register EDP-auditors, *NOREA jaarboek 2000*, NOREA, Amsterdam 1999.

[Koed99]
Mw. drs. M.J.A. Koedijk RA, *Van systeembeoordeling naar procesbeoordeling*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[NIVRA00]
Koninklijk Nederlands Instituut Van Registeraccountants, *Richtlijnen voor Accountantscontrole*, IFAC, Amsterdam, editie 2000.

[NOREA98] Nederlandse Orde van Register EDP-auditors, NOREA-geschrift 1 *IT-auditing aangeduid*, NOREA, Amsterdam 1998.

[Shio01]
T. Shioda, *Het standaardoordeel van de IT-auditor ..., de weg naar eenduidigheid?*, afstudeerscriptie Hanzehogeschool Groningen, februari 2001.

[Praa96]
J. van Praat en H. Suerink, *Inleiding EDP-auditing*, Kluwer Bedrijfswetenschappen, 2e druk, Deventer 1996.

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

Drs. R.J.M. van Langen RA is, na vele jaren in de controlepraktijk bij KPMG, sinds 1997 werkzaam op het brede terrein van IT-auditing. Hij houdt zich daarnaast bezig met de ontwikkeling van vaktechniek binnen KPMG Information Risk Management en heeft Taroh Shioda begeleid bij zijn afstudeeronderzoek.

T. Shioda heeft in het kader van zijn RA-studie aan de Hanzehogeschool Groningen zijn praktijkstage en afstudeeropdracht vervuld bij KPMG Information Risk Management. Hij is thans werkzaam bij KPMG Assurance als trainee in de algemene controlepraktijk.

Mw. drs. M.J.A. Koedijk RA is werkzaam als seniormanager bij KPMG Information Risk Management. Haar werkterrein beslaat naast werkzaamheden ter ondersteuning van de jaarrekeningcontrole voornamelijk proces- en systeembeoordelingen van zowel ERP-pakketten als maatwerksystemen. Zij is verantwoordelijk voor de ontwikkeling van methoden, producten en trainingen op beide werkterreinen en treedt op als docent van interne en externe cursussen.