Internationale standaard voor assuranceopdrachten

Drs. P. Veltman RE RA

In juni 2000 heeft de International Federation of Accountants de definitieve versie van de *International Standard on Assurance Engagements* uitgebracht. Hoewel deze standaard primair bedoeld is voor de beroepsgroep van accountants, zullen IT-auditors er ongetwijfeld mee in aanraking komen. De standaard is ook prima geschikt voor *IT assurance engagements*.

Inleiding

Na een lange voorgeschiedenis heeft de International Federation of Accountants (IFAC) medio 2000 dan eindelijk de *Assurance Engagement*-standaard gepubliceerd. Aanvankelijk *Reporting on the Credibility of Information* genoemd, verschaft deze standaard een breed raamwerk voor zogenaamde assuranceopdrachten. De standaard wordt hierna aangeduid als ISA 100 (International Standard on Auditing).

Assuranceopdrachten zijn opdrachten die tot doel hebben om op basis van onderzoek (het toetsen aan evaluatiecriteria) door een *professional* '*accountant*' een bepaalde mate van zekerheid of geloofwaardigheid te verschaffen inzake een onderzoeksobject. Het onderzoeksobject kan een cijfermatige opstelling zijn maar ook een systeem of proces en zelfs een gedrag. ISA 100 noemt als voorbeelden van dat laatste: corporate governance, het voldoen aan regelgeving en de uitvoering van personeelsbeleid.

Opmerkelijk is dat een IT-systeem of een informatieverwerkend proces niet als voorbeeld wordt genoemd (ISA 100 geeft hier onder meer het voorbeeld van interne controle). Niettemin is er geen enkele reden om te veronderstellen dat ISA 100 niet van toepassing zou zijn op dergelijke onderzoeksobjecten.

De standaard valt globaal in twee delen uiteen:
* een behandeling van de verschillende elementen van een assuranceopdracht;
* een meer uitgebreide en diepgaande behandeling van een *high level assurance engagement* uitgevoerd door een openbare auditor. Op dergelijke opdrachten zijn zwaardere eisen van toepassing.

IFAC-standaarden kennen een brede en nog toenemende internationale acceptatie. In Nederland zijn zij opgenomen in de RAC-bundel (richtlijnen voor de accountantscontrole) en dus van toepassing op de beroepsuitoefening van de registeraccountant.

Voor de beroepsuitoefening van de IT-auditor ligt dit wat minder duidelijk. Het aandeel van registeraccountants in deze beroepsgroep is duidelijk aan het afnemen en bovendien heeft zowel de Register EDP-auditor (RE) als de Certified Information Systems Auditor (CISA) eigen beroepsregels en -standaarden.

Anderzijds zijn veel openbaar optredende RE's en CISA's verbonden aan een (openbaar) accountantskantoor en hebben zij uit dien hoofde te maken met de regelgeving voor de registeraccountant.

Los van de vraag naar de 'jurisdictie' kan ISA 100 op zijn eigen merites worden beoordeeld voor wat betreft geschiktheid voor het IT-auditingberoep. In dit artikel wordt ingegaan op de belangrijkste bepalingen, waarbij voor de term accountant het neutralere auditor wordt gehanteerd. Vervolgens wordt ISA 100 op hoofdlijnen vergeleken met andere regels en standaarden die voor de Nederlandse IT-auditor relevant zijn.

Assuranceopdrachten

De standaard begint met een nadere karakterisering van assuranceopdrachten. Opvallend hierbij is dat termen als *audit*, *review* en *investigation* worden vermeden. De werkzaamheden van de auditor worden getypeerd met de werkwoorden *evaluate* en *measure*, maar als zelfstandig naamwoord wordt uitsluitend *engagement* gebruikt. In dit artikel worden hiervoor de termen *opdracht* en *onderzoek* gehanteerd.

Van een assuranceopdracht zal sprake zijn indien de volgende elementen aanwezig zijn:
a. een tripartiete relatie bestaande uit:
   – een professionele auditor;
   – een verantwoordelijke partij;
   – een beoogde gebruiker;
b. een onderzoeksobject (*subject matter*);
c. geschikte criteria;
d. een proces van opdrachtuitvoering;
e. een conclusie.

Tripartiete relatie

De tripartiete relatie suggereert dat het gaat om een derdenonderzoek (*third party investigation*), maar de verantwoordelijke partij en de beoogde gebruiker kunnen onderdeel uitmaken van dezelfde organisatie.

De opdrachtgever kan zowel de verantwoordelijke partij als de beoogde gebruiker zijn.

Een professionele auditor in de zin van ISA 100 is een auditor die verbonden is aan een firma die lid is van IFAC.

Onderzoeksobject

ISA onderkent drie categorieën van onderzoeksobjecten, maar deze opsomming is niet uitputtend:
* gegevens (zoals historische of prospectieve financiële informatie, performance-indicatoren);
* systemen en processen;
* gedrag.

Het onderzoeksobject kan betrekking hebben op zowel een bepaald moment in de tijd als een tijdsperiode. Het object moet identificeerbaar zijn, evalueerbaar of meetbaar en vatbaar voor het verzamelen van bewijsmateriaal dat de evaluatie of meting ondersteunt.

Criteria

De criteria zijn de toetsingsnormen of benchmarks die worden gebruikt om het onderzoeksobject te evalueren of te meten. Criteria zijn geschikt als zij consistente evaluatie op basis van deskundige oordeelsvorming mogelijk maken. Geschikte criteria zijn verder contextgevoelig, dat wil zeggen relevant in de specifieke opdrachtsituatie.

In het tweede deel van de standaard worden nog wat nadere eisen gesteld aan de criteria. Deze kunnen worden ontleend aan bestaande bronnen (denk aan de Code voor Informatiebeveiliging) of speciaal voor de opdracht zijn ontwikkeld. In beide gevallen zal de auditor moeten nagaan of de criteria geschikt zijn voor de specifieke opdrachtsituatie. Geschikte criteria voldoen aan de volgende eisen:
* *relevant:* van waarde als het gaat om het verbeteren van de kwaliteit van het onderzoeksobject en/of het beslissingsproces van de beoogde gebruiker;
* *betrouwbaar:* consistente evaluatie door verschillende auditors mogelijk makend;
* *neutraal:* niet uitnodigend tot bevooroordeelde conclusies;
* *begrijpelijk:* niet vatbaar voor verkeerde interpretatie;
* *volledig:* alle omstandigheden afdekkend die van invloed kunnen zijn op de conclusie.

Proces van opdrachtuitvoering

De opdrachtuitvoering kent de gebruikelijke stappen van opdrachtaanvaarding, planning, eigenlijke uitvoering en rapportage. Voor IT-auditors (nog) niet te doen gebruikelijk is het voorschrift om – in de planningsfase – materialiteits- en risicoafwegingen te maken. Dit houdt in dat de auditor expliciet inschattingen maakt van het risico dat een materiële tekortkoming over het hoofd wordt gezien, en van de verschillende componenten waaruit dat risico is opgebouwd.

Materialiteit kan volgens ISA 100 in kwalitatieve en kwantitatieve termen worden uitgedrukt en hangt vooral af van de (veronderstelde) belangen van de beoogde gebruiker(s).

Het materialiteitsconcept heeft in het IT-auditingvakgebied nog nauwelijks theoretische fundering. Zoals gezegd speelt het in de praktijk evenmin een grote rol, anders dan in de impliciete afwegingen die de auditor maakt bij zijn deskundige oordeelsvorming.

Het risicomodel wordt in de accountantspraktijk op grote schaal toegepast, al is het niet onomstreden (zie recent nog [Blok01]). In de Nederlandse IT-auditingliteratuur is het model een enkele keer aan de orde gesteld (zie bijvoorbeeld [Mos98] en [Velt95]).

> Het risicomodel houdt in dat de auditor expliciet inschattingen maakt van het risico dat een materiële tekortkoming over het hoofd wordt gezien.

Zoals bekend bestaat het risicomodel (meestal aangeduid als *audit risk model*, maar in deze standaard *engagement risk* genoemd) uit een aantal componenten:
* het *inherente risico* van het optreden van fouten, storingen, onregelmatigheden en andere zaken die afbreuk doen aan het onderzoeksobject;
* het *internecontrolerisico* dat deze leemten niet worden voorkomen of tijdig ontdekt en gecorrigeerd door de getroffen beheersingsmaatregelen;
* het *ontdekkingsrisico* dat de auditor bovengenoemde tekortkomingen niet constateert.

In deze vorm is het model niet zonder meer toepasbaar op assuranceopdrachten die het stelsel van beheersingsmaatregelen als onderzoeksobject hebben. Dit geldt met name voor veel IT-assuranceopdrachten.

Het opdrachtrisico is niet te verwarren met het zakelijk risico van negatieve publiciteit, imago-aantasting, aansprakelijkstelling en dergelijke dat samenhangt met de beroepsuitoefening.

Conclusie

De conclusie geeft met een bepaalde mate van zekerheid weer of het onderzoeksobject in elk materieel opzicht voldoet aan de gestelde criteria.

Was in eerdere conceptversies van de standaard nog sprake van een zekerheidscontinuüm, in de definitieve versie is dit teruggebracht tot drie niveaus (absoluut, hoog en beperkt), waarbij alleen het hoge niveau verder is uitgewerkt. De idee van een zekerheidscontinuüm is nog niet losgelaten, maar aan de praktische uitwerking zitten veel haken en ogen.

Een absoluut niveau van zekerheid zal in de IT-auditingpraktijk niet gauw voorkomen.

Een assuranceopdracht die moet leiden tot een conclusie met een hoog niveau van zekerheid wordt meestal *audit* genoemd, maar zoals gezegd vermijdt (de definitieve versie van) ISA 100 dit soort termen. Een hoog niveau van zekerheid leidt (bij goedkeuring) tot een positief geformuleerde conclusie: ‘Wij zijn van mening dat het onderzoeksobject (in elk materieel aspect) voldoet aan de gestelde criteria’. De definitieve standaard laat zich over de formulering overigens niet meer uit.

Met de term *review* wordt gewoonlijk een opdracht aangeduid die leidt tot een conclusie met een beperkte mate van zekerheid. Een beperkte mate van zekerheid correspondeert met 'plausibel'. Volgens de meeste auditstandaarden moet dit met een negatieve formulering onder woorden worden gebracht: 'Ons is niet gebleken dat het onderzoeksobject niet voldoet aan de gestelde criteria'.

Ten aanzien van de conclusie maakt de standaard verder nog onderscheid tussen een *attest engagement* en een *direct reporting engagement*.
Van een attestopdracht is sprake als de conclusie betrekking heeft op een bewering van de verantwoordelijke partij (een verantwoording). Bij een *direct reporting engagement* heeft de conclusie rechtstreeks betrekking op het onderzoeksobject.
Het onderscheid heeft verder geen consequenties voor de uitwerking van de standaard.

Assuranceopdrachten met een hoge mate van zekerheid

In het tweede deel van de standaard worden verdergaande eisen geformuleerd voor assuranceopdrachten uitgevoerd door een openbare auditor die resulteren in een conclusie met een hoge mate van zekerheid. Een aantal van deze eisen is hierna uitgelicht.

Opdrachtaanvaarding

De auditor moet in schijn en werkelijkheid onafhankelijk zijn. Hij mag een opdracht alleen aanvaarden als aan de volgende voorwaarden is voldaan:
* Het onderzoeksobject moet onder de verantwoordelijkheid vallen van een andere partij. Dit komt bij voorkeur in de opdrachtbevestiging, maar in ieder geval in het rapport ook zo tot uitdrukking.
* De aard van het onderzoeksobject mag een conclusie met een hoge mate van zekerheid niet op voorhand uitsluiten.
* Het onderzoeksteam moet over de vereiste deskundigheid beschikken. Bij het onderzoek mogen zogenaamde experts worden ingeschakeld (zie hierna).

Bewijsmateriaal

De auditor moet voldoende bewijsmateriaal verzamelen om de conclusie op te kunnen baseren. Dit is een nogal voor de hand liggende eis, maar ISA 100 werkt dit nog wat verder uit.

Zo geeft de standaard een aantal vuistregels om de betrouwbaarheid van bewijs te beoordelen:
* Bewijs van externe bronnen is betrouwbaarder dan bewijs dat intern is vervaardigd.
* Intern bewijs is betrouwbaarder als het onderworpen is geweest aan interne controle.
* Bewijs verkregen door de auditor is betrouwbaarder dan bewijs verkregen door de verantwoordelijke partij.
* Bewijs in de vorm van documenten is betrouwbaarder dan mondeling bewijs.
* Bewijs is betrouwbaarder als het afkomstig is uit verschillende bronnen en consistent is.

Verder memoreert de standaard dat het moeilijker is adequaat bewijsmateriaal te verzamelen over een tijdsperiode dan over een tijdstip (werking respectievelijk bestaan). In het algemeen zal de conclusie over de werking van een proces beperkt moeten blijven tot de onderzoeksperiode, en zal geen enkele zekerheid kunnen worden gegeven over de werking in de toekomst.

Gebeurtenissen na de onderzoeksperiode

Het vraagstuk van de gebeurtenissen na de onderzoeksperiode is vooral bekend uit de accountantspraktijk. Het gaat om gebeurtenissen na de afsluiting van het onderzoek maar vóór de (definitieve) rapportering, die de geldigheid van de conclusie kunnen aantasten.

De standaard schrijft voor dat de auditor moet overwegen of op grond van dergelijke gebeurtenissen de conclusie moet worden bijgesteld. Voor de IT-auditingpraktijk kan men denken aan een onderzoek naar de opzet en het bestaan van beveiligingsmaatregelen dat heeft geleid tot een goedkeurende conclusie in het conceptrapport. Wat nu als vervolgens, nog voor het uitbrengen van het definitieve rapport, een geslaagde inbraakpoging plaatsvindt (een materiële verstoring)?

Aangenomen dat het onderzoek goed is uitgevoerd, zijn er twee mogelijkheden:
* Er is sprake van een leemte die niet is ontdekt doordat het onderzoek niet was gericht op het verkrijgen van absolute zekerheid. Met andere woorden, de 'fout' valt binnen de marge tussen hoog en absoluut.
* Er heeft zich na de datum van afsluiting van het onderzoek een wijziging voorgedaan in de omstandigheden (maatregelen buiten werking gesteld, nieuwe bedreigingen) waardoor de conclusie inmiddels haar geldigheid heeft verloren.

Moet de IT-auditor zijn rapport in deze situaties aanpassen en zo ja, hoe? Moet hij aanvullend onderzoek verrichten? De literatuur laat zich hier helaas niet over uit.

Gebruikmaken van het werk van een expert

Niet alleen in de rol van opdrachtverantwoordelijke auditor, maar ook in de rol van expert als lid van het onderzoeksteam kan de IT-auditor met ISA 100 in aanraking komen. De accountant (opdrachtverantwoordelijke auditor) is gehouden zich ervan te vergewissen dat de expert voldoende kennis heeft van de standaard om verband te kunnen leggen tussen zijn aandeel en het doel van de opdracht. De expert die betrokken is bij een assuranceopdracht moet voldoen aan de eisen van ISA 100 en eventuele andere toepasselijke standaarden, zo schrijft ISA 100 voor.

Rapportering

Hoewel de standaard geen voorbeeldteksten meer bevat (in een eerdere conceptversie was dat wel het geval), gaat hij vrij uitvoerig in op het rapport.

Het rapport kan in verschillende vormen worden uitgebracht, zoals een presentatie, een mondelinge bespreking

en een schriftelijk rapport (hard copy en elektronisch). Een schriftelijk rapport is echter het meest effectief.

Het (schriftelijke) rapport dient ten minste te bevatten:

1. Titel.

2. Geadresseerde(n): de partij(en) waaraan het rapport is gericht. Meestal is dit de beoogde gebruiker, maar het rapport kan ook worden geadresseerd aan de verantwoordelijke partij, ter verdere verspreiding.

3. Een beschrijving van de opdracht en van het onderzoeksobject. Deze beschrijving dient ook het doel van de opdracht te omvatten alsmede indien van toepassing de tijdsperiode waarop het rapport betrekking heeft.

4. Een verklaring van de verantwoordelijke partij en de auditor over de wederzijdse verantwoordelijkheden (voor het onderzoeksobject respectievelijk de conclusie).

5. Indien er restricties gelden voor de verspreiding: de partijen waarvoor het rapport is bestemd en het doel waarvoor het is vervaardigd.

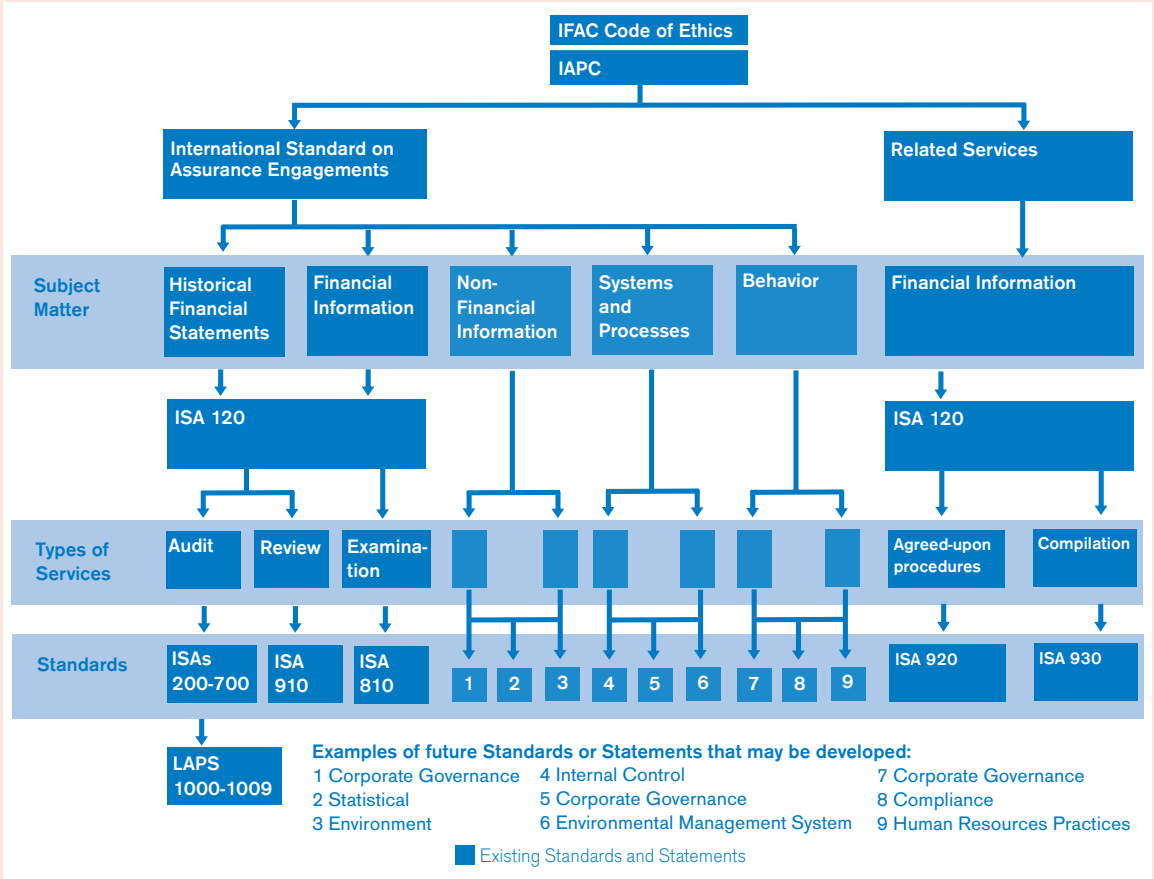
6. Een verwijzing naar de standaard(en) volgens welke de opdracht is uitgevoerd. Minimaal moet dus worden verwezen naar ISA 100. Als een meer specifieke standaard voorhanden is, moet daarnaar worden verwezen (zie figuur 1).

7. Een verwijzing naar de gehanteerde criteria. De criteria kunnen zijn beschreven in (een bijlage bij) het rapport, maar het is ook mogelijk dat wordt volstaan met een verwijzing naar een openbare of althans voor de gebruiker(s) van het rapport toegankelijke bron.
ISA 100 beveelt ook aan dat wordt vermeld of de criteria algemeen aanvaard zijn, gegeven het doel van de opdracht en de aard van het onderzoeksobject.

8. De conclusie. De conclusie wordt gepresenteerd in de vorm van een mening van de auditor over het voldoen van het onderzoeksobject aan de criteria, met een hoge mate van zekerheid. Als de opdracht meerdere doelstellingen had, moeten evenzovele conclusies worden gegeven.
Voor eventuele beperkingen of onthoudingen (zie hierna) moeten de redenen worden vermeld.

9. Rapportdatum. Dit is ook de datum tot welke de auditor eventuele nieuwe ontwikkelingen met een materieel effect op het onderzoeksobject heeft laten meewegen, voorzover hij hiervan op de hoogte was.

10. De naam van de auditor of van de firma en de plaats van uitgifte van het rapport.



Figuur 1. Samenhang IFAC-standaarden.

Conclusie met beperking of onthouding
De auditor moet een beperking (*reservation*) in zijn conclusie aanbrengen of zich van een conclusie onthouden (*denial*) in de volgende omstandigheden:
* Eén of meer aspecten van het onderzoeksobject voldoen niet aan de criteria.
* De verantwoording is ongeschikt in termen van de criteria.
* De auditor heeft niet voldoende bewijs kunnen verzamelen.

In het rapport moeten alle omstandigheden en overwegingen worden vermeld die hebben geleid tot de beperking of onthouding.

Overige informatie
In het rapport mogen andere informatie en toelichtingen worden opgenomen die niet bedoeld zijn als een beperking. Als voorbeelden noemt ISA 100: specifieke bevindingen, aanbevelingen en verwijzingen naar inherente beperkingen van het onderzoeksobject. Deze aanvullende informatie mag niet zodanig zijn verwoord dat de strekking van de conclusie wordt aangetast.

Verhouding met andere standaarden

Voor de Nederlandse IT-auditor zijn vooral de reglementen van NOREA, ISACA en NIVRA/IFAC relevant. In deze paragraaf worden de NOREA- en ISACA-reglementen op een aantal punten met ISA 100 vergeleken. Deze vergelijking beperkt zich tot de officiële reglementen en richtlijnen; studierapporten, geschriften en dergelijke blijven derhalve buiten beschouwing.

Beknopte inhoudelijke vergelijking

NOREA
De IT-auditor die is ingeschreven in het register van NOREA is bij zijn beroepsuitoefening gehouden aan de gedrags- en beroepsregels, het reglement beroepsbeoefening en de verzameling richtlijnen ([NOREA92], [NOREA94] respectievelijk [NOREA99]).

De richtlijnen bestaan op dit moment uit De Richtlijnen voor de Attestfunctie, waarin zijn opgenomen: opdrachtformulering en -aanvaarding; dossiervorming en -beheer; en rapportage.

Bij een globale inspectie van deze richtlijnen in vergelijking met ISA 100 valt het volgende te constateren:
* NOREA gaat uit van een tweepartijenmodel van opdrachtgever en opdrachtnemer, waardoor de verschillende rollen van verantwoordelijke partij en beoogde gebruiker niet zo goed uit de verf komen.
* NOREA besteedt betrekkelijk weinig aandacht aan de onderzoekscriteria, maar dit kan nog komen in de aangekondigde richtlijn over uitvoering van werkzaamheden.
* Zaken als materialiteit, risicoanalyse en mate van zekerheid komen (nog) niet aan bod. NOREA besteedt evenmin aandacht aan mogelijke nuanceringen in de conclusie.
* Onderwerpen als de onweerlegbaarheid van de vermelding van de identiteit van de IT-auditor, de duurzaamheid van het medium waarop het rapport is vastgelegd en de onmogelijkheid om het rapport ongemerkt te kunnen veranderen, worden door NOREA betrekkelijk uitvoerig behandeld.

ISACA
De *standards*, *statements* en *guidelines* van de Information Systems Audit and Control Association zijn aanzienlijk uitgebreider en verder uitgewerkt dan die van NOREA. ISACA bestaat dan ook al wat langer en beschikt over meer middelen.

ISACA kent behalve een *Code of Professional Ethics* een verzameling *IS Auditing Standards* (met een verplicht karakter) en een verzameling *IS Auditing Guidelines* (waarvan gemotiveerd kan worden afgeweken). Verder kent ISACA een verzameling standaarden voor *control professionals*.

Helaas ontbreekt een algemene standaard op het niveau van ISA 100, waardoor vergelijking wordt bemoeilijkt. Duidelijk is wel dat ISACA de IT-auditor meer handvatten biedt voor de dagelijkse beroepsuitoefening dan IFAC, maar dat komt ook doordat IFAC nog niet is toegekomen aan de invulling van *Systems and Processes* (zie figuur 1).

Zo kent ISACA een richtlijn met handreikingen om materialiteitsafwegingen te maken ([ISACA99]) en een richtlijn voor de risicoafweging ([ISACA00]). De rapportagerichtlijn [ISACA98] besteedt aandacht aan gebeurtenissen na de onderzoeksperiode, zonder overigens antwoord te geven op de eerder gestelde vragen.

Vrijwel al de elementen die ISA 100 behandelt komen in de ISACA-standaarden en -richtlijnen in meer detail aan bod. Een essentiële zaak als de mate van zekerheid in de conclusie ontbreekt echter. Gezien de wildgroei aan benamingen als *quick scan*, *quick review* en *benchmark*, naast de traditionele maar vaak als synoniem gebruikte *audit* en *review*, is daar juist dringend behoefte aan.

Reikwijdte en geldigheid

De praktiserende IT-auditor dient zich vanzelfsprekend te houden aan de reglementen die de beroepsvereniging hanteert waarvan hij lid is. In Nederland zijn de meeste IT-auditors lid van NOREA, maar combinaties van RE-CISA en RE-RA komen ook veel voor. Bij een samenloop zal de auditor aan meerdere regelingen moeten voldoen. Gelukkig is er, voorzover uit de literatuur en op grond van de beknopte inhoudelijke vergelijking kan worden opgemaakt, geen sprake van onoverkomelijke conflicten tussen de verschillende regelingen.

Veel IT-auditors zijn werkzaam bij openbare accountantskantoren. In de meeste gevallen moeten zij, ongeacht hun professionele kwalificatie(s), voldoen aan de relevante accountantsregelgeving, al dan niet in de rol van expert.

Gezag

Zonder twijfel genieten de IFAC-standaarden internationaal het meeste gezag in het maatschappelijk verkeer. In Nederland geldt dat waarschijnlijk ook, al zullen de RE-beroepsbeoefenaren meer gezag toekennen aan de NOREA-reglementen.

De ISACA-standaarden zijn behalve bij de leden (CISA's) weinig bekend en zoals het spreekwoord zegt: 'Onbekend maakt onbemind'.

Samenvatting en conclusie

Na een draagtijd van meer dan vijf jaar en ampele discussies en consultaties heeft IFAC het licht doen zien aan een breed raamwerk voor assuranceopdrachten, kortweg *Assurance Engagements* genoemd. Een assuranceopdracht is een opdracht die resulteert in een opinie van een professionele auditor over het voldoen van een onderzoeksobject aan de onderzoekscriteria met een bepaalde mate van zekerheid.

De standaard weerspiegelt het streven van de accountantsberoepsgroep om het werkterrein van financial auditing uit te breiden met diensten als milieu-auditing en operational auditing. In dit licht is het merkwaardig dat IT als onderzoeksobject niet expliciet wordt genoemd, temeer daar de accountantsprofessie al wel producten als WebTrust en SysTrust op de markt heeft gezet.

De standaard weerspiegelt het streven van de accountantsberoepsgroep om het werkterrein van financial auditing uit te breiden.

Hoewel de standaard op onderdelen wat minder baanbrekend is dan de eerdere concepten, is het toch een resultaat dat er mag wezen. De standaard is weliswaar niet zo uitgebreid en gedetailleerd als de ISACA-standaarden en -richtlijnen, maar wel vaktechnisch gedegen en zeker bruikbaar voor de IT-auditingprofessie. Bovendien is het een gezaghebbende standaard, waar IT-auditors hoe dan ook nog veel mee te maken zullen krijgen.

Literatuur

[Blok01]
Prof. J.H. Blokdijk RA, *De effectiviteit van de systeemgerichte aanpak in de accountantscontrole*, Maandblad voor Accountancy en Bedrijfseconomie, maart 2001.

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

[Gort01]
Prof. J.C.A. Gortemaker, *International Standard on Assurance Engagements*, Maandblad voor Accountancy en Bedrijfseconomie, maart 2001.

[ISACA98]
Report Content and Form, Information Systems Audit and Control Association, 1 december 1998.

[ISACA99]
Materiality Concepts for Auditing Information Systems, Information Systems Audit and Control Association, 1 september 1999.

[ISACA00]
Use of Risk Assessment in Audit Planning, Information Systems Audit and Control Association, 1 september 2000.

[Mos98]
T.O. Mos CISA RE RI, *Het (accountants?) audit-risk voor IT-auditing beschouwd*, de EDP-Auditor, nr. 3, 1998.

[NOREA92]
Reglement Gedrags- en Beroepsregels Register EDP-auditors, Nederlandse Orde van Register EDP-Auditors, 1992.

[NOREA94]
Reglement Beroepsbeoefening Register EDP-auditors, Nederlandse Orde van Register EDP-Auditors, 1994.

[NOREA98]
IT-auditing aangeduid, NOREA geschrift nr. 1, Nederlandse Orde van Register EDP-Auditors, 1998.

[NOREA99]
Richtlijnen, Nederlandse Orde van Register EDP-Auditors, jaarboek 1999 addendum.

[NOREA00]
Handleiding ZekeRE Business, Nederlandse Orde van Register EDP-Auditors, ongedateerd.

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

Drs. P. Veltman RE RA is sinds 1983 werkzaam in het openbare auditingberoep en heeft ervaring opgedaan met zowel financiële controles als het gehele scala aan IT-auditopdrachten. Bij KPMG Information Risk Management houdt hij zich onder meer bezig met vaktechniek en quality assurance.