Toezicht financiële sector in Nederland

Dit artikel heeft als doel om een overzicht te geven van de ontwikkelingen ten aanzien van de regelgeving bij de diverse toezichthouders voor de financiële instellingen in Nederland en de impact daarvan op de werkzaamheden van de IT-auditor. Hierbij zal onder meer worden aangegeven wat de regelgeving inhoudt en wat er nu gewijzigd is ten opzichte van de oude situatie en wat de gevolgen hiervan zijn voor de financiële instellingen. In het algemeen kan gesteld worden dat de beheersing van ICT een steeds belangrijker onderdeel gaat vormen in de regelgeving van toezichthouders. Dit artikel zal met name ingaan op de IT-specifieke issues die voortvloeien uit de regelgeving. Verschillende auteurs hebben aan dit artikel hun bijdrage geleverd.

Ontwikkelingen in toezicht financiële sector

In Nederland is vooralsnog een aantal toezichthouders aanwezig, waaronder De Nederlandsche Bank (DNB), de Stichting Toezicht Effectenverkeer (STE) en de Stichting Pensioen- & Verzekeringskamer (PVK). DNB heeft naast haar taken met betrekking tot de euro en op het gebied van het betalingsverkeer, ook een andere hoofdtaak, namelijk het toezicht op banken, het toezicht op beleggingsinstellingen en het toezicht op wisselkantoren. De STE houdt zich bezig met het toezicht op de effectenhandel in Nederland, beschermt de positie van de belegger en zorgt voor het goed en doorzichtig functioneren van markten. De PVK ten slotte houdt toezicht op de in Nederland werkzame verzekeringsmaatschappijen en pensioenfondsen. Bovengenoemde drie toezichthouders werken samen in de Raad voor Financiële Toezichthouders (RFT) ([RFT00]) met als doel de coördinatie en afstemming van niet-sectorspecifieke regelgeving en beleid te intensiveren. Deze samenwerking werd mede ingegeven door de verdergaande ontwikkelingen in de financiële marktsector, zoals de ontwikkeling van financiële conglomeraten en de voortgaande vervlechting van financiële producten. Een voorbeeld hiervan is de fusie van de beurzen van Amsterdam, Brussel en Parijs, die zijn samengevoegd in Euronext. Aangezien elk land zijn eigen toezichthouders heeft, kan de vraag worden gesteld welke regelgeving van toepassing zal zijn voor Euronext. Voorlopig zal in elk geval nog gelden dat de regelgeving landspecifiek is.

Ook internationaal bestaat een instelling, namelijk de Bank for International Settlements (BIS), die actief is op het gebied van regelgeving ten aanzien van financiële instellingen, zoals e-commerce principles en kapitaalsrichtlijnen, die beter bekendstaan onder de verzamelnaam 'Bazel II'. De BIS is een internationaal opererende organisatie die zich voornamelijk bezighoudt met het onderzoek op het gebied van het internationale monetaire beleid en financiële samenwerking. Verder fungeert de BIS als bank voor de nationale centrale banken.

Ten aanzien van de drie toezichthouders DNB, STE en PVK zijn reeds gedurende enkele maanden ontwikkelingen en discussies vanuit de overheid gaande om het huidige toezichtmodel te herzien. 'Kern van het voorstel is dat het sectorale toezicht op banken, effecteninstellingen en verzekeraars grensoverschrijdend wordt. De Nederlandsche Bank (DNB) en de Pensioen- & Verzekeringskamer (PVK) gaan zich toeleggen op het bedrijfseconomische (prudentieel) toezicht van financiële instellingen. De Stichting Toezicht Effectenverkeer krijgt het gedragstoezicht, en wordt omgevormd tot de Financiële Markten Autoriteit (FMA).'[1] ([FinD01]). Kortom, turbulentie alom! In tabel 1 is een overzicht gegeven van de recente ontwikkelingen.

Gesteld kan worden dat toezichthouders qua regelgeving voortdurend in beweging zijn en dat dit derhalve ook impact heeft op de werkwijze binnen de financiële sector en sectoren daarbuiten, waaronder de externe accountants en IT-auditors. In de afgelopen periode hebben we gezien dat op het gebied van regelgeving nieuwe dan wel gewijzigde regelgeving tot stand is gekomen en in werking is getreden. Voorbeelden hiervan zijn de 'Regeling Organisatie en Beheersing' van DNB (per 1 april 2001) ([DNB01]) en de 'Wijziging Nadere Regeling toezicht effectenverkeer 1999' (met ingang van 1 september 2001). Hierna zal verder op deze gewijzigde regelgeving worden ingegaan.

DNB/PVK	STE
Samenwerking zal worden geïntensiveerd	Alle financiële instellingen
Bevordert sectoroverschrijdende benadering van conglomeraten	Gericht op goede omgang onderling en met de consument
DNB krijgt prudentieel toezicht op effecteninstellingen (van STE)	STE krijgt gedragstoezicht op beleggingsinstellingen (van DNB)
	Ontwikkeling tot Financiële Markten Autoriteit (FMA[1])
	Vanaf 2002 verantwoordelijk voor Financiële Bijsluiter en andere vormen van consumentenvoorlichting

Tabel 1. Overzicht recente ontwikkelingen ([Hoog01]).

1) Voor wat betreft de nieuwe naam van de nieuwe toezichthouder (FMA of AFM) willen wij een voorbehoud in dit artikel maken.

Regeling Organisatie en Beheersing (ROB) van De Nederlandsche Bank

Mw. B. Beugelaar RE RA

Inleiding

De ROB is in werking getreden met ingang van 1 april 2001. Om financiële instellingen niet per direct te belasten met de invoering van deze regelgeving heeft DNB een overgangstermijn gesteld van één jaar. De totstandkoming van de ROB werd mede ingegeven door de diverse soorten van bestaande circulaires en het Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen uit 1988. Daarnaast gold dat door de ontwikkelingen op het gebied van corporate governance, de toenemende mate van aandacht voor compliance en integriteit, alsmede het bestaan van diverse 'sound practices', zoals de Code voor Informatiebeveiliging, een wijziging van de bestaande regelgeving noodzakelijk was. Bij het opstellen van de ROB is getracht om de mate van detaillering in de regelgeving te beperken en de uiteindelijk inhoudelijke invulling aan de sector over te laten. Eén van de pluspunten bij de totstandkoming van de ROB is dat deze in samenwerking met de vertegenwoordigers van de financiële sector (Nederlandse Vereniging van Banken (NVB)) en het Koninklijk NIVRA (Nederlands Instituut van Register Accountants) is opgesteld.

Mede naar aanleiding van de invoering van de ROB is door het NIVRA een Audit Alert 11 opgesteld waarin, onder consultatie van DNB, is aangegeven welke werkzaamheden van de accountant worden verwacht inzake de ROB. Het betreft hier een tijdelijke handreiking. De kenmerken van deze Audit Alert 11 worden verderop in het artikel nog behandeld.

Wijzigingen en kenmerken naar aanleiding van de invoering van de ROB

Eén van de belangrijkste wijzigingen is dat de ROB één omvattende regeling is die de volgende zeven richtlijnen en aanbevelingen vervangt:
* Administratieve organisatie bij kredietinstellingen;
* Organisatie valuta-arbitrage;
* Risicobeheer derivaten bij kredietinstellingen;
* Memorandum inzake het toezicht van de Bank op het renterisico;
* Memorandum betreffende specifieke aspecten van de rol van de Raad van Commissarissen in het bankwezen;
* Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen;
* Brief en considerans inzake uitbesteding van de geautomatiseerde gegevensverwerking.

Voor de IT-auditor waren de twee laatstgenoemde richtlijnen altijd van belang bij het uitvoeren van de werkzaamheden op het gebied van de informatietechnologie (IT). Deze richtlijnen zijn in de ROB vervangen en qua omvang aanzienlijk gereduceerd. De IT-richtlijnen in de ROB worden gevormd door een inleiding en een viertal artikelen, te weten:

* Artikel 54: *De instelling beschikt over helder geformuleerde beleidsuitgangspunten ter beheersing van IT-risico's. De beleidsuitgangspunten worden vastgelegd en gecommuniceerd aan alle relevante geledingen van de instelling.*
* Artikel 55: *De instelling voert op systematische wijze een analyse van IT-risico's uit. De analyse wordt uitgevoerd zowel op instellingsbrede basis als op het niveau van de onderscheiden bedrijfsonderdelen.*
* Artikel 56: *De instelling draagt zorg voor de uitwerking en implementatie van de beleidsuitgangspunten ter beheersing van IT-risico's in zichtbare organisatorische en administratieve procedures en maatregelen, welke geïntegreerd zijn in de IT-processen en de dagelijkse werkzaamheden van alle relevante geledingen. Tevens wordt voorzien in een systematisch toezicht op de naleving daarvan.*
* Artikel 57: *De instelling draagt zorg voor specifieke maatregelen die een afdoende beveiliging van de informatie en de continuïteit van de IT waarborgen. De rechtszekerheid en de privacy van de cliënten dienen bij gebruikmaking van IT-toepassingen in voldoende mate te zijn gewaarborgd.*

De artikelen 58 tot en met 64 behandelen de uitbesteding van (delen van) bedrijfsprocessen, waaronder ook de IT-uitbesteding is begrepen. Ook bij uitbesteding geldt dat een instelling dient te beschikken over een helder geformuleerd beleid, een risicoanalyse dient uit te voeren en technische en organisatorische maatregelen en procedures dient te treffen ter beheersing van de risico's. Tevens moet door de instelling een schriftelijke overeenkomst (service level agreement) inzake de uitbesteding worden opgesteld, waarbij geldt dat mogelijkheden gecreëerd zijn om controles en toezicht uit te voeren door zowel DNB als externe accountants op de door de dienstverlener verrichte activiteiten. Expliciet wordt gesteld dat het niet is toegestaan om de interne auditfunctie uit te besteden aan een niet tot de groep behorende instelling en de financiële administratie en het opstellen van de jaarrekening uit te besteden aan de controlerende externe accountant.

Verder staat binnen de regeling de separate aandacht voor de verantwoordelijkheid van het bestuur en de commissarissen centraal. Dit betekent dat het bestuur en de commissarissen primair verantwoordelijk zijn voor het te voeren beleid en de invulling van de regeling. Doordat de regeling op hoofdlijnen is gesteld, geeft deze ook meer vrijheid voor de instelling voor wat betreft de concrete invulling van de regeling. De financiële instelling dient hier op een verstandige wijze mee om te gaan. Hierbij wordt opgemerkt dat ondanks de vrijheid qua invulling hierop een toetsing door de toezichthouder zal plaatsvinden.

In de Regeling Organisatie en Beheersing zijn de richtlijnen voor de IT-auditor qua omvang aanzienlijk gereduceerd.

Daarnaast betreft de regeling een uitwerking op hoofdlijnen waarbij getracht is om de mate van detaillering te beperken en bevat zij derhalve een framework met minimumvereisten.

IT-risico	Beoordelingscriteria
Strategisch risico	Het betreft hier het inherente risico als gevolg van het ontbreken van een adequate IT-strategie en een adequaat IT-beleid. Beoordelingscriteria hierbij zijn: * de mate waarin het IT-beleid aansluit op de bedrijfsdoelstellingen; * het wel/niet aanwezig zijn van een IT-beleid en de kwaliteit daarvan; * de mate van volledigheid van het IT-beleid en de IT-strategie en de aansluiting daarvan op de bedrijfsdoelstellingen; * de mate waarin het IT-beleid en de IT-strategie worden uitgedragen door de organisatie en worden ondersteund door het ter beschikking stellen van voldoende middelen (mensen, financieel, technisch).
Beheersbaarheids-risico	Het betreft hier het inherente risico als gevolg van complexe en inflexibele informatie- en technische systemen dat afbreuk doet aan het adequaat beheersen van deze systemen. Beoordelingscriteria hierbij zijn: * de mate van onderhoudbaarheid en flexibiliteit van de systemen. Bijvoorbeeld de mate waarin de functionaliteit in een informatie-systeem eenvoudig kan worden aangepast; * de benodigde tijdsduur voor het uitvoeren van wijzigingen in systemen; * de mate van flexibiliteit van de systemen.
Exclusiviteitsrisico	Het betreft hier het inherente risico als gevolg van het kunnen verkrijgen/hebben van ongeautoriseerde toegang tot informatie en informatiesystemen. Beoordelingscriteria hierbij zijn: * de mate van toereikendheid van de logische en fysieke toegangsprocedure; * de mate van het zich voordoen en de frequentie van incidenten als gevolg van ongeautoriseerde toegang (bijvoorbeeld fraude); * de mate waarin de incidenten door externe dan wel interne tekortkomingen zich hebben voorgedaan. Naar onze mening dient hierbij ook gedacht te worden aan het informatiebeveiligingsbeleid.
Integriteitsrisico	Het betreft hier het inherente risico als gevolg van onjuiste, onvolledige of niet-tijdige informatie. Beoordelingscriteria hierbij zijn: * de mate en frequentie van het zich voordoen van onjuiste, onvolledige en niet-tijdige informatieverstrekking (bijvoorbeeld fouten in vaste gegevens); * het wel/niet voldoen aan regelgeving; * de mate van tijdigheid van opleveren van rapportages en informatie.
Controleerbaar-heidsrisico	Het betreft hier het inherente risico als gevolg van niet-adequate beheersings- en controlemogelijkheden ten aanzien van de IT. Beoordelingscriteria hierbij zijn: * de mate waarin het functioneren van de systemen kan worden getest, dan wel in het verleden reeds is getest; * de mate waarin internecontrolemaatregelen zijn vastgelegd en ingevoerd; * de mogelijkheden tot het uitvoeren van bepaalde controles op bepaalde (vastgestelde) momenten; * de kwaliteit van procedures betreffende: - systeemontwikkeling; - testen; - change management; - problem management; - configuration management; - performance management.
Continuïteitsrisico	Het betreft hier het inherente risico als gevolg van discontinuïteit in de geautomatiseerde gegevensverwerking. Beoordelingscriteria hierbij zijn: * de mate waarin en frequentie waarmee zich verstoringen voordoen in de geautomatiseerde gegevensverwerking (bijvoorbeeld systeem- en netwerkstoringen); * de benodigde tijd om storingen op te lossen en de productie te herstarten; * het wel/niet aanwezig zijn van uitwijk- en back-upmaatregelen.
Gebruikersrisico	Het betreft hier het inherente risico als gevolg van het niet-adequate gebruik van de IT. Beoordelingscriteria hierbij zijn: * de mate waarin adequaat gebruik wordt gemaakt van de IT (ondersteuning aan gebruikersorganisatie en IT-organisatie); * de ervaring en opleiding van de gebruikers van informatie-systemen en technische systemen; * de mate van gebruiksvriendelijkheid van informatie- en technische systemen voor zowel opgeleide als niet-opgeleide gebruikers; * de wijze waarop geautomatiseerde procedures gerelateerd kunnen worden aan handmatige procedures.

Tabel 2. Beoordelingscriteria per IT-risico.

Een ander belangrijk aandachtspunt vanuit de regeling is dat de risicobeheersing van bedrijfsprocessen centraal staat. Dit kan worden afgeleid van artikel 1, waarin de goede sturing en beheersing van de bedrijfsprocessen en de beheersing van de risico's die de instelling loopt, worden aangegeven. Door DNB is ten behoeve van het uitoefenen van toezicht een Handboek Risicoanalyse opgesteld. Deze risicoanalyse wordt door DNB gehanteerd bij het uitvoeren van toezicht op de onder toezicht staande banken, onder meer voor het opsporen van hoge inherente risico's en zwakke risicobeperkende beheersingsmaatregelen en om bij haar werkzaamheden de nadruk te leggen op die banken, of activiteiten binnen banken, met een slecht risicoprofiel. Deze risicoanalyse en de daaruit voortvloeiende beoordelingscriteria kunnen ook door de instellingen worden gebruikt ter ondersteuning bij het opstellen van de risicoanalyse. De DNB-risicoanalyse wordt ten behoeve van het opstellen van een IT-risicoanalyse in de volgende paragraaf nader uitgewerkt.

Risicoanalyse DNB

In deze paragraaf zal met name worden ingegaan op de voor het uitwerken van de IT-risicoanalyse specifieke punten. In de ROB wordt een zevental specifieke IT-risico's genoemd, te weten strategisch, beheersbaarheids-, exclusiviteits-, integriteits-, controleerbaarheids-, continuïteits- en gebruikersrisico. Het is derhalve van belang om hieraan bij het uitvoeren van de risicoanalyse aandacht te schenken.

In de risicoanalyse van DNB wordt onder IT-risico verstaan: *'IT risk is the current or prospective risk to earnings and capital arising from inadequate information technology and processing in terms of manageability, exclusivity, integrity, controllability and continuity. Further, IT risk arises from an inadequate IT strategy and policy and from inadequate use of the information technology.'*

In tabel 2 volgen kort per specifiek IT-risico enkele beoordelingscriteria vanuit de DNB-risicoanalyse ([DNB]), welke kunnen worden meegenomen bij het opzetten van de risicoanalyse.

Aan artikel 55 en 60 van de ROB wordt voldaan door voor bovenstaande specifieke IT-risico's een risicoanalyse uit te voeren. Hierbij dient bedacht te worden dat bovenstaande opsomming van beoordelingscriteria niet limitatief is en dat afhankelijk van de omvang en complexiteit van de IT-organisatie en het belang hiervan voor de bedrijfsprocessen de lijst van criteria nog kan worden aangevuld.

Impact van regelgeving voor de financiële instelling en voor de werkzaamheden van de IT-auditor

De invoering van de ROB betekent voor de IT-auditor dat de belangrijkste artikelen inzake IT zijn gereduceerd tot een aantal artikelen, een inleiding en een tweetal paragrafen in de ROB. Voor de IT-auditor zijn van belang de artikelen 54, 55, 56 en 57. De artikelen inzake de uitbesteding van (delen van) bedrijfsprocessen, waaronder ook de IT-uitbesteding kan vallen, zijn gereduceerd tot een zevental. Qua aard van de te verrichten

auditwerkzaamheden is er voor de IT-auditor echter niet veel veranderd. Voor de instelling geldt dat DNB meer de nadruk legt op het door de instelling expliciet vastleggen van het IT-beleid en de risicoanalyse. Dit laatste leidt er echter wel toe dat in de audits, meer dan nu het geval is, (ook) kan worden getoetst tegen beleidsregels van de instelling zelf.

De werkzaamheden van de IT-auditor zullen zich met name richten op de volgende aspecten:

* Een toetsing en beoordeling op hoofdlijnen van de door de organisatie uitgevoerde assessment in hoeverre wordt voldaan aan de ROB voor wat betreft de IT-aspecten, dient plaats te vinden. Het betreft hier een toetsing en beoordeling van de opzet en het bestaan van de betreffende organisatie-inrichting en het beheersingsmechanisme. Hierbij treedt een verandering op ten opzichte van de oude situatie in die zin dat de instelling nu verplicht is de eigen beoordeling in hoeverre wordt voldaan aan de regelgeving expliciet te beschrijven. De instellingen worden nu als het ware gedwongen om het IT- en beveiligingsbeleid en de IT-risicoanalyse concreet uit te werken. Deze beschrijving en interne assessment kan de IT-auditor als normering hanteren bij zijn IT-auditactiviteiten, mits deze IT-risicoanalyse en het IT-beleid van een voldoende niveau zijn.

* De externe IT-auditor zal bij zijn werkzaamheden zoveel mogelijk trachten te steunen op de door de interne IT-auditor reeds uitgevoerde werkzaamheden. Hierin treedt derhalve geen wijziging op ten opzichte van de oude situatie.

* Tekortkomingen en gebreken dienen schriftelijk te worden gerapporteerd in een management letter of in een of meer separate rapportages. Een management letter in de vorm van een powerpoint-presentatie wordt door DNB niet als toereikend ervaren ([Koni01]). Derhalve dient een adequate beschrijving van de aangetroffen tekortkomingen en gebreken te worden opgenomen. Ook hiervoor geldt dat dit ook reeds in de oude situatie van toepassing was.

* Minimaal moet er worden gerapporteerd over de bevindingen inzake de beheersing van de IT-risico's en majeure afwijkingen. Een algeheel oordeel omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking behoeft derhalve niet te worden verstrekt. Ook hierbij treedt geen verandering op ten aanzien van de oude situatie.

* Door DNB wordt verwezen naar 'sound practices' als toetsingscriteria. Hierbij geldt als voordeel dat regelgeving minder onderhoudsgevoelig is als gevolg van bijvoorbeeld toekomstige technologische ontwikkelingen ([Osse01]). Door IT-auditors worden als toetsingscriteria onder meer de Code voor Informatiebeveiliging en CobIT van ISACA gehanteerd. Deze standaarden kunnen de IT-auditor ondersteunen bij de advisering aan zijn cliënten omtrent op te zetten beheersingsmaatregelen. Afhankelijk van de omvang van de instelling en de afhankelijkheid van de IT dient hier door de instelling in meerdere of mindere mate invulling te worden gegeven aan het opzetten van beheersingsmaatregelen ter reductie van de IT-risico's. De mate van detaillering van invulling mag door de instelling zelf worden bepaald; hierbij geldt echter wel dat een adequaat onderbouwde analyse aanwezig dient te zijn ter beheersing van de IT-risico's. De IT-auditor zal een beoordeling uitvoeren op de door de instelling opgeleverde risicoanalyse en de daarbij gehanteerde 'sound practices'.

Door het Koninklijk NIVRA is naar aanleiding van de invoering van de ROB een Audit Alert 11 ([NIVR01]) uitgegeven. In deze uitgave is opgenomen dat door de accountant/IT-auditor de volgende aspecten dienen te worden meegenomen:

* Aanbeveling: rapporteren in de management letter 2001 over de status (voortgang) betreffende de implementatie van de ROB bij de betrokken instelling. Dit geldt alleen voor het boekjaar 2001, dat uiterlijk eindigt per 31 maart 2002.

* 'Door de instelling dient aan de externe accountant een opdracht ter toetsing en beoordeling van de ROB te worden gegeven. Dit is dus een opdracht die anders is dan de opdracht tot controle van de jaarrekening. In feite is hier sprake van een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden. Dat deze werkzaamheden in belangrijke mate zullen samenvallen met de werkzaamheden die noodzakelijk zijn in de context van de jaarrekeningcontrole (hetgeen overigens niet steeds het geval behoeft te zijn), doet niet af aan de noodzaak om deze additionele opdracht zelfstandig in een opdrachtbevestiging vast te leggen. Dit kan gebeuren als onderdeel van (c.q. aanvulling op) de opdrachtbevestiging die wordt gehanteerd voor de jaarrekeningcontrole of in een afzonderlijke opdrachtbevestiging.'

* 'Het wordt niet noodzakelijk geacht in de opdrachtbevestiging een (uitvoerige) opsomming van de te verrichten werkzaamheden op te nemen. Volstaan kan worden met de mededeling dat de werkzaamheden zullen worden verricht die voortvloeien uit artikel 23 van de ROB en die in de Audit Alert 11 nader zijn omschreven.'

Concluderend kunnen we stellen dat DNB, mede door het beperken van de detaillering in de ROB, de instellingen vrijheid geeft ten aanzien van de wijze van invulling en evaluatie in hoeverre wordt voldaan aan de artikelen in de ROB. DNB geeft hierbij aan dat gebruikgemaakt kan worden van de op IT-gebied beschikbare 'sound practice'-publicaties met betrekking tot risicobeheersing. Aangezien deze 'sound practices' zich dynamisch zullen ontwikkelen als gevolg van veranderingen in de markt, zal dit ook doorwerken in de op te leveren IT-risicoanalyse, het IT-beleid, het informatiebeveiligingsbeleid en de te treffen beheersingsmaatregelen. Voor de IT-auditor betekent het hanteren van 'sound practices' dat op basis van 'professional judgement' beoordeeld zal worden of organisaties de juiste afweging hebben gemaakt bij de invulling van hun risicoanalyse en IT- en informatie-

Figuur 1. Stappenplan van werkzaamheden in het kader van de ROB.

Mw. B. Beugelaar RE RA is als manager werkzaam bij KPMG Information Risk Management binnen de Line of Business Financial Services. In deze functie heeft zij een brede ervaring opgedaan in de financiële dienstverlening aan met name bancaire instellingen. Zij heeft rollen vervuld op het gebied van onder meer regelgeving van de financiële toezichthouders, informatiebeveiliging, projectmanagement van pakketimplementaties, het opzetten en beoordelen van internecontrolestructuren en het beoordelen van bank- en betaalsystemen. Verder is zij verantwoordelijk voor de productontwikkeling binnen IRM Financial Services.

beveiligingsbeleid. De jaarlijkse werkzaamheden voor de instelling en IT-auditor om te bepalen in hoeverre wordt voldaan aan de ROB zullen met name bestaan uit de in figuur 1 weergegeven stappen.

De gegevensverzameling zal met name door de instelling zelf worden uitgevoerd. Hierbij dienen activiteiten te worden verricht waarbij gegevens verzameld en vastgelegd worden ter ondersteuning van het uitvoeren van de analyse. Ook het uitvoeren van de selfassessment zal met name door de organisatie zelf worden uitgevoerd. Wel kan de IT-auditor hierbij ondersteuning verlenen, bijvoorbeeld ten aanzien van het opstellen en identificeren van IT-beheersingsmaatregelen uit hoofde van 'sound practices'. Als resultaat van de analyse zal een rapportage van bevindingen worden opgesteld op basis waarvan verbeteracties gedefinieerd dienen te worden. Ook hierbij kan de IT-auditor op grond van zijn kennis omtrent IT-beheersingsvraagstukken ondersteuning in de vorm van advisering geven. Uiteindelijk zal een finale toetsing dienen plaats te vinden in hoeverre de organisatie voldoet aan de ROB. Daarbij zal onder meer een beoordeling van de door de instelling opgeleverde IT-risicoanalyse en het IT-beleid worden uitgevoerd. De finale toetsing zal door de IT-auditor worden verricht, met als resultaat een separate rapportage of management letter. Een verandering ten opzichte van de oude situatie is met name dat door DNB expliciet gesteld is dat instellingen de IT-risicoanalyse en het IT-beleid en informatiebeveiligingsbeleid dienen te beschrijven en dat de IT-auditor hiervan gebruik kan maken bij zijn toetsing en auditwerkzaamheden.

Nadere regelgeving effectenverkeer door de Stichting Toezicht Effectenverkeer

Drs. H.G.Th. van Gils RE RA

Inleiding

De Stichting Toezicht Effectenverkeer (STE) heeft als belangrijkste taken het bevorderen van een adequate functionering van effectenmarkten en het bevorderen van de bescherming van beleggers tegen malafide aanbiedingen, onvoldoende informatie en ondeskundig optreden. Om dat te ondersteunen heeft de STE een aantal regels opgesteld waaraan de instellingen zich dienen te houden en waaraan het verkrijgen c.q. houden van de vergunning is gekoppeld. De meest concrete daarvan is de Nadere Regeling toezicht effectenverkeer 1999 (NR1999), die in 2001 is gewijzigd en aangevuld door de Wijziging Nadere Regeling toezicht effectenverkeer 1999. In het vervolg van deze paragraaf zal vooral op deze twee documenten worden ingegaan.

Voor internettoepassingen is de 'Beleidsnotitie 99-0003 inzake het Internet in relatie tot het toezicht op het effectenverkeer in Nederland' van toepassing. Deze is reeds uitgebreid in Compact besproken. Daarom wordt hier eenvoudigheidshalve verwezen naar [Beug00].

Nadere Regeling toezicht effectenverkeer 1999

Door de Nadere Regeling toezicht effectenverkeer 1999 (NR1999) wordt een groot aantal regels gegeven aan instellingen om bovenstaande doelstellingen te effectueren. Vooral paragraaf 7, regels met betrekking tot de administratieve organisatie en interne controle, is voor accountants en IT-auditors van belang. Deze paragraaf kent slechts één artikel:

Artikel 24
1. *Een effecteninstelling beschikt, met het oog op het adequaat functioneren van de effecteninstelling en de naleving van de wettelijke vereisten*[2]*, over een adequate administratieve organisatie en een systeem van interne controle overeenkomstig de regels in bijlage 4.*

2. *De in het eerste lid bedoelde administratieve organisatie en het systeem van interne controle worden op systematische wijze beschreven, regelmatig geëvalueerd en zo nodig geactualiseerd.*

Per 1 september 2001 is de Wijziging Nadere Regeling toezicht effectenverkeer 1999 van kracht geworden. Deze wijziging van de NR1999 heeft aan dit artikel een derde lid toegevoegd:

3. *Een effecteninstelling meldt aan de STE iedere voorgenomen significante wijziging van de in het eerste lid genoemde administratie en systeem van interne controle.*

Deze laatste toevoeging lijkt ingrijpender dan het is. In het Besluit toezicht effectenverkeer 1995 was deze bepaling reeds opgenomen, echter zonder de kwalificatie 'significant'. In de praktijk werd dit natuurlijk al wel als zodanig toegepast.

In bijlage 4 van de NR1999 staan in 27 artikelen concrete regels voor de inrichting van de administratieve organisatie en interne controle. Diverse artikelen bevatten voor accountants en IT-auditors relevante aanwijzingen, met name gericht op de application controls. Voor de general IT-controls gaat alle aandacht uit naar artikel 4.27 'Geautomatiseerde systemen'. Voor een indicatie van de regels wordt verwezen naar tabel 3. Deze tabel bevat niet de letterlijke tekst uit de regeling, maar geeft met slechts enkele steekwoorden zoveel mogelijk de strekking van de regels weer. Daarbij blijken ook duidelijk de aanvullingen die door de Wijziging NR1999 zijn aangebracht.

2) In de Wijziging Nadere Regeling toezicht effectenverkeer 1999 is de zinsnede 'naleving van de wettelijke vereisten' vervangen door 'naleving van bij of krachtens de wet gestelde vereisten'.

Door de Wijziging NR1999 wordt het eerste lid als volgt gespecificeerd:

Artikel 4.27 lid 1
De effecteninstelling die gebruikmaakt van geautomatiseerde gegevensverwerking dient zodanige maatregelen en procedures door te voeren dat de beveiliging (vertrouwelijkheid, integriteit en continue beschikbaarheid) van de geautomatiseerde gegevensverwerking is gewaarborgd. Daarbij dient aandacht te zijn besteed aan maatregelen op de volgende gebieden:
a. algemene beheersmaatregelen in de geautomatiseerde omgeving;
b. de gehanteerde functiescheidingen;
c. geprogrammeerde controles die zich richten op de betrouwbare werking van de gebruikte applicaties ('application controls'); en
d. de maatregelen in de gebruikerscontroles.

In de toelichting op de wijzigingen wordt gesteld dat de realisatie van de uitwerking van artikel 4.27 dient te geschieden met inachtneming van de algemeen geaccepteerde normen zoals de Code voor Informatiebeveiliging en CobIT van ISACA. Voor internettoepassingen wordt als norm aangehouden de Handleiding ZekeRE Business van de NOREA.

Nieuw is de regel dat de instelling moet zorgen voor een plannings- en evaluatiecyclus, die voortdurend bewaakt of de juiste maatregelen zijn getroffen en waaruit de werking van het beleid blijkt. De periodieke evaluatie van het beveiligingsbeleid dient te zijn gebaseerd op actuele risicoanalyses (art. 4.27.5). Dit laatste sluit aan op de algehele tendens om voor een beter begrip van effectiviteit van maatregelen te toetsen aan risicoanalyses (zie ook de paragraaf over de ROB van De Nederlandsche Bank).

Impact van regelgeving voor organisatie en werkzaamheden van IT-auditor

De NR1999 geeft een compacte opsomming die een goed kader vormt voor te treffen maatregelen. Organisaties die voor de inrichting al min of meer aansloten op de standaarden, zoals de Code voor Informatiebeveiliging of CobIT, zullen in het algemeen weinig moeite hebben om aan de regels te voldoen. Wellicht dat, in navolging van de ROB-wijziging van DNB, het verplicht uitvoeren van risicoanalyses nieuw is. Organisaties die zowel onder het toezicht van DNB als van de STE vallen, zullen in het algemeen met dezelfde maatregelen voor beide toezichthouders goed uit de voeten kunnen.

De regels zijn in zekere zin formeel te noemen. Dit is mede nodig om de getroffen maatregelen ook te kunnen toetsen. In de controleaanpak van de STE wordt primair uitgegaan van de eigen verantwoordelijkheid van de instellingen en wordt waar mogelijk gesteund op de werkzaamheden van de interne accountantsdiensten en externe EDP-auditors. Opvallend is dat in de toelichting van de Wijziging NR1999 expliciet staat opgenomen dat beoordeling van de IT-specifieke onderdelen van de geautomatiseerde bedrijfsprocessen door gecertificeerde EDP-auditors dient te worden uitgevoerd. Uit een samenvatting van de regelingen van de verschillende internationale Security Boards, verenigd in de International Organization of Securities Commissions (IOSCO), blijkt dat onder gecertificeerde EDP-auditors de bij NOREA ingeschreven Register EDP-auditors worden bedoeld ([IOSC01]).

Artikel (verwijzing)	Aandachtsgebied (geen letterlijke tekst van NR1999) (cursief gedrukte tekst is nieuw volgens de Wijziging NR1999 vanaf 1 september 2001)
4.27.1	Zie tekst in dit artikel
4.27.2.1	Programmatuur: - voorkomen ongeautoriseerde wijzigingen in programmatuur (lid a) - functiescheiding ontwikkel/testomgeving van productieomgeving (lid b) - testen van nieuwe programmatuur (lid c)
4.27.2.2	Problem management
4.27.2.3	Operations management
4.27.3	Logische toegangsbeveiliging: - op basis van competentietabellen (die de fysieke functiescheiding in de organisatie waarborgen) (lid a) - beheer competentietabellen en wachtwoorden (lid b en c) - opnemen van geprogrammeerde (invoer)controles (lid d) - *herstelprocedure voor invoerfouten (lid e)*
4.27.4	Continuïteit: - herstelprocedures na calamiteit of storing (lid a) - gebruikershandleiding (lid b) - back-upprocedures (lid c) - uitwijkprocedures (lid d) - beveiliging gegevensdragers en computerfaciliteiten (lid e)
4.27.5	*Beveiligingsbeleid op basis van risicoanalyse en periodieke evaluatie (zie opmerking in tekst)*
4.27.6	*Aanpassingen in systemen mede baseren op veranderingen doelstelling en risicoprofiel van de instelling*

Tabel 3. STE-regelgeving geautomatiseerde systemen.

Beoordeling van de IT-specifieke onderdelen van de geautomatiseerde bedrijfsprocessen dient door een gecertificeerde EDP-auditor te worden uitgevoerd.

Een bijzondere situatie doet zich voor als delen van de automatisering zijn uitbesteed. Op dit moment is er nog geen specifieke richtlijn of beleidsnotitie door de STE gepubliceerd, maar uit praktijksituaties blijkt wel dat de STE ervan uitgaat dat de instelling verantwoordelijk is voor de hele verwerkingsketen, dus inclusief de beveiliging van de verwerking bij derde partijen. Op de een of andere manier dient de instelling zich er dus van te vergewissen dat de automatisering van de externe verwerkingsorganisatie aan minimaal de eisen van de NR1999 en de Beleidsnotitie Internet 99-0003 voldoet. Uit de praktijk blijkt dat alleen een service level agreement met afspraken over het gewenste beveiligingsniveau onvoldoende is. Op de een of andere manier moet tevens vastgesteld worden dat de externe verwerkingsorganisatie zich ook daadwerkelijk aan die beveiligingsregels houdt. In Nederland wordt daar in de praktijk de third-party-mededeling, afgegeven door een onafhankelijke EDP-auditor, voor gebruikt. Internationaal lijkt SAS70 daarvoor het aangewezen instrument. Voor internetdiensten heeft de STE expliciet aangegeven dat slechts toestemming wordt verleend indien door een onafhankelijke Register EDP-auditor onderzoek is gedaan naar de gehele keten, dus ongeacht welke automatiseringsorganisaties daarbij (waar ter wereld ook) zijn betrokken. Zoals

Drs. H.G.Th. van Gils RE RA
is als senior manager in de service line Financial Services werkzaam bij KPMG Information Risk Management. Hij is bij veel financiële instellingen betrokken geweest op het gebied van kwaliteitsbeheersing en beoordeling van financiële applicaties en technische infrastructuur.

eerder is aangegeven, heeft de STE voor dergelijke audits geen concreet normenkader uitgewerkt. De auditor zal dit zelf moeten doen met in het achterhoofd de eerder in dit artikel genoemde bronnen van normenstelsels.

Daarbij vereist de STE in eerste instantie een mededeling van de IT-auditor gericht op de opzet van de beveiligingsmaatregelen. Als de STE van oordeel is dat voldoende (beveiligings)maatregelen zijn getroffen, krijgt de organisatie toestemming om de internetdienst te starten. Vervolgens eist de STE dat door de EDP-auditor na drie maanden een onderzoek wordt gedaan naar het bestaan van de eerder in opzet beoordeelde maatregelen. Voor een beoordeling van de werking wordt geen afzonderlijke mededeling meer vereist. De STE gaat ervan uit dat de werking in de reguliere IT-audits, zoals die ook voor de niet-internetgerelateerde diensten worden uitgevoerd, zal worden meegenomen.

Toezicht door de Pensioen- & Verzekeringskamer

Drs. P.C.J. van Toledo RE RA

Algemeen

De Pensioen- & Verzekeringskamer (PVK) houdt toezicht op de in Nederland werkzame verzekeringsmaatschappijen en pensioenfondsen. Het doel hiervan is zorgen dat deze instellingen financieel gezond zijn én blijven, en dat zij ook in de toekomst aan hun verplichtingen kunnen voldoen.

De PVK werkt met een normatief toezichtsysteem. Dat wil zeggen dat de PVK volgens vooraf gestelde normen zich een oordeel vormt over de onder toezicht staande instellingen. Door inzage in en overleg over jaarlijkse verslagstaten en bijvoorbeeld accountantsverslagen komt dit oordeel tot stand. De PVK voert tevens speerpuntonderzoeken uit, waarbij dieper wordt ingegaan op één specifiek onderwerp. Verder is de toetsing van alle nieuwe en zittende bestuurders en directeuren van verzekeraars en pensioenfondsen op deskundigheid en betrouwbaarheid een belangrijke taak. De nadruk ligt de komende jaren op integriteit, (internationale) samenwerking tussen de financiële toezichthouders, conglomeraatvorming en het toezicht daarop, transparantie en informatieverstrekking. Daarnaast is er op dit moment veel aandacht voor consumentenvoorlichting en vernieuwing van bestaande beleidsregels voor financiële toetsing.

Het beleid dat de PVK voert is tweeledig. Enerzijds past de PVK de bestaande toezichtswetgeving toe. Voor de uitoefening van het toezicht van de PVK zijn de PSW (pensioenfondsen), de WTV'93 en WTN (verzekeringsmaatschappijen) de belangrijkste wetten. Anderzijds hanteert zij de eigen PVK-bevoegdheden bestaande uit Voorschriften, Beleidsregels en Aanbevelingen. Voorschriften zijn de meest dwingende bevoegdheden. Aanbevelingen daarentegen hebben geen verplicht karakter.

Beheersing van ICT

Ten aanzien van de beheersing van risico's uit hoofde van ICT heeft de PVK geen specifieke voorschriften of richtlijnen uitgevaardigd. Het toezicht van de PVK richt zich vooral op de financiële en actuariële opzet van de onder toezicht staande instellingen en de inhoud van de statuten en reglementen. Bij de uitoefening van het toezicht is de kwaliteit van de ICT en de beheersing van ICT een aandachtsgebied, met name voor wat betreft bijzondere issues zoals euroconversie en millenniumwisseling. Zo heeft de PVK zich continu een beeld gevormd van de millenniumproblematiek bij de aangesloten instellingen. Hetzelfde geldt voor de europroblematiek. Aan de beheersing van ICT in zijn algemeenheid is tot op heden weinig aandacht besteed. Ook in de recent uitgevaardigde Principes voor Interne Beheersing (PIB) wordt slechts in beperkte mate ingegaan op de beheersing van ICT.

Zoals in de voorgaande paragraaf is aangegeven, verkrijgt de PVK de informatie over informatiebeveiliging grotendeels uit de management letters en rapportages aan de RvC naar aanleiding van de jaarrekeningcontrole. Deze informatieverstrekking is voor verzekeringsmaatschappijen vastgelegd in de Drie-partijen-overeenkomst tussen PVK, verzekeraar en certificerend accountant. De accountant en de daarbij ingeschakelde IT-auditor vervullen hierdoor een belangrijke rol in de informatieverstrekking inzake de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking aan de PVK. Indertijd heeft men de aangesloten instellingen specifiek gevraagd om de accountant in de management letter aandacht te laten besteden aan de millenniumproblematiek. Hierbij dient opgemerkt te worden, dat voor de jaarrekeningcontrole niet beschreven is welke werkzaamheden de accountant (de IT-auditor) ten aanzien van ICT moet (laten) uitvoeren.

Meldingsplicht

Indien een IT-auditor is ingeschakeld door de certificerend accountant, kan hij te maken krijgen met de meldingsplicht, die is vastgelegd in de Drie-partijen-overeenkomst tussen PVK, verzekeraar en accountant en in de Pensioen- en Spaarfondsenwet. De meldingsplicht is van toepassing op de certificerend accountant bij verzekeringsmaatschappijen en de certificerend accountant en actuaris bij pensioenfondsen. Het betreft uitsluitend werkzaamheden die in het kader van de controle van de jaarrekening en verslagstaten worden uitgevoerd. De meldingsplicht is van toepassing in de volgende situaties:

* In strijd met de PVK-eisen voor (verkrijgen) vergunning;
* Omstandigheden die het voortbestaan van de onderneming bedreigen;

* In strijd met de bij wet opgelegde verplichtingen;
* Omstandigheden die leiden tot weigering van afgeven goedkeurende accountantsverklaring.

De IT-auditor kan bij zijn reguliere werkzaamheden voor de jaarrekeningcontrole worden geconfronteerd met het ontbreken of het ernstig tekortschieten van continuïteitsvoorzieningen voor de geautomatiseerde gegevensverwerking of hij kan bij zijn werkzaamheden ernstige leemten in de AO/IC aantreffen. Na constatering zullen de bevindingen in overleg met de verantwoordelijke accountant tot melding moeten leiden aan de PVK.

Hierbij moet opgemerkt worden, dat er op dit moment bij de actuarissen en de accountants nog de nodige vragen bestaan over de invulling van de meldingsplicht en welke normen 'wanneer is het ernstig' hierbij moeten worden gehanteerd. Enkele belangrijke vragen in dit kader zijn:
* Welke controlewerkzaamheden mag de PVK van de accountant/actuaris verwachten tijdens de controle van jaarrekening en verslagstaten?
* Mag de onderneming in de gelegenheid worden gesteld om de omstandigheid te verhelpen? Mag de onderneming het initiatief nemen tot overleg met de PVK?
* Op welke termijn moet de continuïteit worden beoordeeld in het geval het voortbestaan van de onderneming wordt bedreigd? Met welke mate van waarschijnlijkheid?

Ontwikkelingen in het toezicht bij de PVK

In maart 2001 heeft de PVK de Principes Interne Beheersing (PIB) voor pensioenfondsen, verzekeringsmaatschappijen en natura-uitvaartverzekeraars in concept uitgebracht. De PVK geeft hierbij invulling aan de bevoegdheid om eisen te stellen aan de AO/IC van verzekeringsmaatschappijen en pensioenfondsen, gebaseerd op artikel 70 WTV respectievelijk Nota van Toelichting van het Koninklijk Besluit van 21 november 2000 omtrent de inhoud van de ABTN. De PIB's hebben vanaf 1 januari 2002 de status van een richtlijn en vallen derhalve onder de voorschriften van de PVK. De PVK geeft aan dat op een later tijdstip voor (een deel van) de primaire processen en ondersteunende processen nadere voorschriften worden opgesteld. Het opzetten van de PIB's voor zowel pensioenfondsen als verzekeringsmaatschappijen is een voortzetting van de lijn om basisrichtlijnen voor het totale PVK-toezichtveld op te stellen. De principes zijn op een hoog abstractieniveau geschreven en zijn toepasbaar voor organisaties van diverse grootte, waardoor de PIB voor pensioenfondsen van toepassing is voor zowel het ABP, het op twee na grootste pensioenfonds, als een klein ondernemingspensioenfonds. Bij de opstelling van de PIB's is aansluiting gezocht bij de bestaande 'sound practices' op het gebied van interne beheersingsmethoden, zoals COSO en corporate governance.

In de PIB's wordt beperkt aandacht geschonken aan de beheersing van ICT. Opvallend is, dat ten aanzien van ICT geen verwijzing wordt gemaakt naar de Code voor Informatiebeveiliging of CobIT. Daarnaast wordt er geen aandacht besteed aan een belangrijk onderwerp als outsourcing. Met name pensioenfondsen maken veel gebruik van uitbesteding van het vermogensbeheer en de administratie. In de PIB voor pensioenfondsen en verzekeringsmaatschappijen wordt uitsluitend aangegeven, dat bij gebruikmaking van ICT de instelling er zorg voor dient te dragen dat de continuïteit en de betrouwbaarheid van de gegevensverwerking zijn gewaarborgd. Een calamiteitenplan dient inzicht te geven in hoe de instelling de continuïteit van de gegevensverwerking waarborgt. In de concept-richtlijn inrichting AO/IC natura-verzekeraars met 50.000 of minder verzekerden van juli 2001 gaat de PVK verder. Hierin worden minimumeisen neergelegd voor automatisering. In deze beschrijving worden eisen gesteld aan de vastlegging van het automatiseringsbeleid, aanschaf van hardware en software, onderhoud, documentatie van maatwerk, toegang tot programma's en bestanden, back-upprocedures, rapportage aan het bestuur inzake wijzigingen en de werking van de IT.

In de PIB voor pensioenfondsen en verzekeringsmaatschappijen wordt specifiek ingegaan op de naleving van de PIB. In de PIB staat vermeld, dat de instelling periodiek en systematisch de effectiviteit van de interne beheersingsmaatregelen toetst. Van de rapportage wordt vermeld dat deze, indien de toetsing plaatsvindt door de interne accountantsdienst dan wel via verbijzonderde interne controle of anderszins, rechtstreeks geschiedt aan het bestuur/de directie en de RvC.

Drs. P.C.J. van Toledo RE RA
is als senior manager werkzaam bij KPMG Information Risk Management en heeft zich gespecialiseerd in de financiële dienstverlening aan met name verzekeringsmaatschappijen en pensioenfondsen. Hij heeft een brede ervaring opgedaan bij bedrijfsbrede implementaties van verzekerings- en pensioenadministratiesystemen. De rollen lagen op het terrein van pakketselecties, quality assurance, projectreviews en het opzetten en beoordelen van internecontrolestructuren. Verder is hij verantwoordelijk voor de productontwikkeling van IRM op het gebied van pensioenfondsen en verzekeringsmaatschappijen.

De aandacht voor ICT in de wet- en regelgeving vanuit de Pensioen- & Verzekeringskamer is nog steeds beperkt.

Met de introductie van de PIB's en de meldingsplicht is de wet- en regelgeving wederom aangescherpt. Ook valt op dat de PVK meer aansluiting zoekt bij bestaande 'sound practices' op het gebied van interne beheersing. Ondanks de sterk toegenomen afhankelijkheid van ICT bij pensioenfondsen en verzekeringsmaatschappijen is de aandacht voor ICT in de wet- en regelgeving vanuit de PVK nog steeds beperkt. De inzet van een IT-auditor is nergens verplicht gesteld.

Afhankelijk van de mate waarin de PVK naleving vereist zijn hier mogelijkheden voor de IT-auditor voor aanvullende dienstverlening. Om te voldoen aan de eisen van de PIB en de nog nader te definiëren eisen aan primaire en ondersteunende processen kan de interne of externe IT-auditor worden gevraagd mee te werken met het opstellen en implementeren van een internal control framework. Verder zou een IT-auditor gevraagd kunnen worden om op basis van risicoanalyse een IT-auditplan op te stellen en vervolgens periodiek een evaluatie uit te voeren op de effectieve werking van de AO/IC en hierover te rapporteren aan het bestuur/de directie en de RvC.
Ten aanzien van de meldingsplicht zou de IT-auditor door de accountant kunnen worden gevraagd om expliciet de continuïteit van de geautomatiseerde gegevensverwerking te beoordelen. Ten aanzien van dit laatste is de individuele accountant vrij de hulp van de IT-auditor al of niet in te roepen.

Regelgeving Bank for International Settlements

Drs. R.P. Schouten RE RA

Inleiding

In voorgaande paragrafen is ingegaan op de in Nederland bekende toezichthouders zoals De Nederlandsche Bank, de Pensioen- en Verzekeringskamer en de Stichting Toezicht Effectenverkeer. Op internationaal gebied is de Bank for International Settlement (hierna: de BIS) voor het bankwezen zeer belangrijk. De door de BIS opgestelde regelgeving wordt door de nationale toezichthouders op het bankwezen nagenoeg een op een onderschreven. Dit maakt de door de BIS uitgeschreven toezichtsrichtlijnen interessant voor in Nederland opererende financiële instellingen. Om deze reden wordt de rol van de BIS in deze paragraaf verder uitgewerkt.

De BIS is een internationaal opererende organisatie die zich voornamelijk bezighoudt met het onderzoek op het gebied van het internationale monetaire beleid en de financiële samenwerking. In aanvulling op het uitvoeren van onderzoek fungeert de BIS tevens als bank voor de nationale centrale banken. De bancaire diensten bestaan specifiek uit activiteiten voor beheersing van vreemde valuta en de goudvoorraad van de centrale banken. Verder voert de BIS vermogensbeheer uit voor de internationale financiële instituten. Het dienstenaanbod richt zich uitsluitend tot de centrale banken en financiële instituten. Het is de BIS niet toegestaan om diensten aan te bieden aan particulieren en grote bedrijven.
Om bovenstaande taken uit te oefenen, initieert de BIS de volgende activiteiten:
* een forum dat discussies en besluitvormingsprocessen tussen de centrale banken en binnen de internationale financiële wereld bevordert en coördineert;
* een centraal orgaan voor economisch en monetair onderzoek;
* het vervullen van de functie van belangrijke tegenpartij voor nationale centrale banken bij het uitvoeren van financiële transacties;
* het vervullen van een intermediaire rol of vertrouwensrelatie bij omvangrijke internationale financieringsactiviteiten.

De documenten die voortkomen uit de discussies en besluitvormingsprocessen van de BIS geven belangrijke richtlijnen voor de nationale toezichthouders, zijnde de nationale centrale banken.
Een groot verschil in de rol ten opzichte van die van de centrale banken wordt gevormd door het feit dat de richtlijnen van de BIS niet op directe maar op een indirecte wijze een belangrijke rol vervullen in de door de (centrale) banken op te zetten normen. De reikwijdte van de normstelling door de BIS beperkt zich niet tot alleen het geven van richtlijnen voor het te voeren beleid, maar strekt zich ook uit tot normen voor de opzet en het beheer van de ICT. Met name deze laatste richtlijnen kunnen van belang zijn voor de door de IT-auditor uit te voeren audit- en advieswerkzaamheden.

Organisatie van The Bank for International Settlements en wijze van totstandkoming van richtlijnen

Voor een goed begrip over de status en het gezag van de uitgebrachte richtlijnen wordt kort stilgestaan bij de totstandkoming van de richtlijnen. De BIS kent de onderstaande commissies:
* Meetings of the Board of Directors;
* Meetings of the Group of Ten (G10) central bank Governors and their subcommittees;
* Meetings of central bank Governors.

In de reguliere gang van zaken stellen de commissies tijdelijke subcommissies in om conceptrichtlijnen voor te bereiden. De commissies voeren een eerste beoordeling uit op de door de subcommissie opgestelde conceptrichtlijn. Indien de conceptrichtlijn van voldoende kwaliteit is, wordt deze uitgestuurd naar de belanghebbenden, zoals de nationale centrale banken en (groot)banken voor commentaar. Vaak worden de conceptrichtlijnen voorzien van een commentaarperiode. Na afloop van de commentaarperiode worden alle commentaren verzameld en na een belangenafweging verwerkt in de definitieve richtlijn.

Relatief veel richtlijnen zijn afkomstig van de G10 en haar subcommissies. De subcommissies zijn door de G10 ingesteld om de onderlinge samenwerking tussen de toezichthouders te bevorderen en beleidsbeslissingen en regelgeving meer in detail voor te bereiden. Dit betreffen:
* The Basel Committee on Banking Supervision;
* Committee on Payment and Settlement Systems;
* Committee on the Global Financial System;
* Committee on Gold and Foreign Exchange.

Hierna volgt per commissie een korte toelichting van haar doelstelling. Tevens is voor de beeldvorming een aantal (concept)richtlijnen ter illustratie opgenomen, alsmede is aangegeven welke commissies nu van belang zijn voor wat betreft richtlijnen en – dit geldt uitsluitend voor de eerste twee – welke impact zij hebben op de werkzaamheden van de IT-auditor.

The Basel Committee on Banking Supervision
Het Basel Committee heeft als doel zoveel mogelijk het toezicht op het bankwezen te uniformeren, teneinde de solvabiliteit en stabiliteit van het internationale bankwezen te bevorderen. Een zeer belangrijke richtlijn op dit gebied is het 'Basel Capital Accord' uit 1988. In dit akkoord is de eerste set richtlijnen opgesteld voor het berekenen van de minimumsolvabiliteit van een bank en richtlijnen voor het minimum aan te houden eigen vermogen tegenover activa.

Bazel II
Inmiddels zijn er nieuwe (concept)kapitaalsrichtlijnen opgesteld die bekend zijn onder de verzamelnaam 'Bazel II'. Bazel II heeft tot doel de interne risicobeheersing binnen het bankwezen te verbeteren. Bazel II verandert de solvabiliteitstoetsing van de banken in die zin dat er nu niet alleen in kwantitatieve zin wordt getoetst maar ook in kwalitatieve zin. De toetsing gaat geschieden aan de hand van de volgende drie toetsingspijlers: vermogen, toezicht en toelichting in algemene zin. Onderstaande

opsomming geeft in hoofdlijnen weer wat binnen de drie toetsingspijlers moet zijn geregeld voor een gezond bankbedrijf:

* vermogen:
  - uitvoeren van interne beheersing van risico's;
  - gebruik van modellen om risico's (kwantitatief) in beeld te krijgen;
  - bepalen van solvabiliteit;
  - periodiek rapporteren aan de toezichthouders;
* toezicht:
  - toezicht meer richten op het beoordelen van het interne proces voor beheersing van de risico's, in plaats van het reguliere toezicht door middel van de beoordeling van de kwantitatieve gegevens in de maandstaatrapportages;
  - meer kwalitatief gericht toezicht, onder andere door beoordeling van competenties van bestuurs- en directieleden;
  - meer zelfstandig uitvoeren van reviews door de toezichthouders zelf;
* toelichting in algemene zin:
  - meer inzicht bieden in de interne risicobeheersing.

In de bovenstaande opsomming staan de termen risico en risicobeheersing centraal. Een belangrijk punt binnen Bazel II betreft het identificeren, maar vooral ook het kwantificeren van risico's (risk measurement). Een belangrijke wijziging ten opzichte van het eerste Basel Accord betreft de aandacht voor het operationele risico naast de reeds bekende risico's zoals het krediet- en marktrisico. Bazel II verplicht de banken om vermogen aan te houden om potentiële verliezen uit hoofde van de operationele bedrijfsvoering te kunnen opvangen. De reden waarom 'pas' nu de vermogenseis voor operationeel risico naar voren is gekomen, komt voort uit het feit dat banken steeds meer (risicovolle) diensten verlenen naast het oorspronkelijke bankbedrijf (waarin vooral het managen van het krediet- en marktrisico centraal staat). Voorbeelden van dienstverlening betreffen de op provisie gebaseerde activiteiten zoals cashmanagement, garantiestellingen en het verstrekken van letters of credit. Verder betreden de banken steeds meer de terreinen zoals securisatie en ook outsourcing van bedrijfsprocessen (bijvoorbeeld van het hypotheekbedrijf of het betalingsverkeer).
Volgens Bazel II is het operationele risico als volgt gedefinieerd:
Het risico van een direct of indirect verlies dat voortkomt uit inadequate of falende interne processen, medewerkers en systemen, of voortkomend uit externe gebeurtenissen.

Gegeven de steeds toenemende integratie van processen en ICT zijn de status van de IT controls en de informatiebeveiliging belangrijke indicatoren om te bepalen wat het niveau van de operationele risico's is.

Om de operationele risico's te kwantificeren en de gevolgen daarvan te meten, zijn de volgende zaken noodzakelijk:

* ontsluiten van (historische) gegevens/data;
* meten van de werkelijk geleden verliezen;
* inschatten van mogelijke huidige/acute verliezen.

Om inzicht te krijgen in de mate van invloed die Bazel II heeft op het uitvoeren van IT-auditwerkzaamheden zijn onderstaand een paar voorbeelden opgenomen. Deze voorbeelden betreffen het kredietrisico en het marktrisico. Zij illustreren tevens wat de mogelijke effecten zijn voor de IT-audit inzake het operationeel risicobeheer.

Ontsluiten van (historische) gegevens/data
Dat het ontsluiten van gegevens niet eenvoudig is, illustreren we aan de hand van een voorbeeld met betrekking tot het kredietrisico. Het is niet ondenkbeeldig dat een vergelijkbare situatie zich ook kan voordoen op het vlak van het operationele risico.
Het voorbeeld gaat over de recente deconfiture van energiegigant Enron.
Door de vele bankfusies en daardoor veelal de complexiteit in systemen die binnen de (groot)banken aanwezig zijn, is het aanleveren en aggregeren van gegevens/data voor de banken zeer arbeidsintensief, of zelfs economisch onhaalbaar geworden. Kort na de bekendwording van het mogelijke faillissement van Enron bleken diverse bankinstellingen niet in staat tijdig betrouwbare informatie over de totale kredietverstrekking aan deze partij uit de eigen systemen op te leveren. Nadat door de diverse woordvoerders en bestuursleden aan de financiële media een totaal potentieel verliesbedrag was verkondigd, bleek later dat de werkelijke verliezen nog groter waren dan gedacht. De gegevens bleken incompleet te zijn. Uit diverse subsystemen kwam pas in tweede instantie informatie omtrent andere kredietverstrekkingen die aanvankelijk niet bekend was.

Meten van werkelijk geleden verliezen
Het voorgaande voorbeeld over Enron is tevens een voorbeeld van het meten van verliezen. Een ander voorbeeld van het kwantificeren van risico's en de daaruit voortvloeiende (mogelijke) verliezen wordt gevonden in het toepassen van modellen voor het bepalen van het marktrisico. De markten (waaronder effecten-, geld-, kapitaal- en valutatermijnmarkt) waarop de banken opereren zijn volatiel. Met behulp van modellen kan worden benaderd wat de gevolgen zijn van de veranderingen in de diverse marktposities. De modellen bevatten onder meer (econometrische) formules, aannames en trends om de berekening van voorspellende waarden te kunnen uitvoeren. Een belangrijke voorwaarde voor een juiste berekening van de voorspellende waarden is dat de (geaggregeerde) input in de modellen voldoende betrouwbaar is. Voor deze (geaggregeerde) input worden vaak posities gebruikt. Voorbeelden van posities zijn: de hoeveelheid aandelen XYZ voor eigen rekening, de kredietomvang aan multinational ABC en de hoeveelheid uitstaande renteswaps. Vanuit allerlei bancaire (sub)systemen dienen gegevens te worden aangeleverd over de afzonderlijke posities om op een geaggregeerd niveau de nettoposities te berekenen.

Als laatste geven wij het voorbeeld van een bank die probeert de werkelijk geleden verliezen te meten inzake beveiligingsincidenten van (bijna gelukte) inbraakpogingen via het internet. Per incident wordt gekeken wat de gemiddelde kosten zijn geweest om het incident te verhelpen om daarmee een voorspellende waarde te krijgen voor de toekomst.

Inschatten mogelijke huidige/acute verliezen
In de situatie dat modellen of formules niet kunnen worden gebruikt, schrijft Bazel II voor om kwalitatieve (op basis van menselijke beoordeling) of andere maatregelen te hanteren om inschattingen te maken.

Samenvattend kan worden gesteld dat het vastleggen van gegevens over bijvoorbeeld beveiligingsincidenten en het niveau van beveiliging, het ontsluiten van gegevens uit de (bancaire) systemen en het op een juiste wijze aggregeren (meten) van gegevens cruciaal is in het operationele risicobeheer. Het beoordelen van het niveau van beveiliging maar ook de techniek inzake het ontsluiten van de gegevens raakt direct de IT-audit.

3) 26 november 2001.

Andere zaken die door de invoering van de richtlijnen volgens Bazel II grote gevolgen voor de IT-audit hebben, zijn:
* de rapportages aan de toezichthouder (betrouwbaarheid);
* de managementrapportages (betrouwbaarheid);
* IT in termen van:
  – dataopschoning;
  – dataontsluiting;
  – inrichting en invoering van modellen;
  – data-aanlevering;
  – capaciteit;
* verandering en aanpassing van processen in de organisatie;
* bemensing in kwantitatieve en kwalitatieve zin.

Mede aan de hand van de gegeven voorbeelden wordt duidelijk waar de toegevoegde waarde van de IT-auditor ligt. Vooral op het gebied van het beoordelen van delen van de operationele, met name aan ICT gerelateerde risico's, de gegevensbenadering en gegevensrapportering kan de IT-auditor waarde toevoegen door het uitvoeren van onderzoeken. Voor de organisatie zelf wordt het ook steeds belangrijker om de IT controls en de informatiebeveiliging op orde te hebben omdat deze factoren rechtstreeks invloed hebben op het vermogensbeslag en daarmee op de resultaten. Het kwaliteitsaspect betrouwbaarheid speelt een belangrijke rol in de normen volgens de richtlijnen van Bazel II.

Vooral op het gebied van gegevensbenadering en gegevensrapportering kan de IT-auditor waarde toevoegen.

De doelstelling van de BIS is dat de banken uiterlijk in 2005 hun interne organisatie zodanig hebben opgezet en ingericht dat wordt voldaan aan de richtlijnen volgens Bazel II. Verwacht mag worden dat de eisen van Bazel II ook hun effect zullen hebben op andere financiële instellingen, zoals bijvoorbeeld assetmanagers die deel uitmaken van financiële concerns. Door de bancaire fusies van de afgelopen jaren en de aard, omvang en complexiteit van de bancaire systemen wordt verwacht dat er de komende jaren grote en zeer complexe projecten gestart zullen worden voor het vastleggen en ontsluiten van risico-informatie. In sommige gevallen mag ook verwacht worden dat bepaalde activiteiten (processen dan wel ICT) meer zullen worden geoutsourced naar een gespecialiseerde partij die de risico's al op een zeer laag niveau heeft gebracht. De betrokkenheid van de IT-auditor bij deze projecten, bijvoorbeeld in de rol van quality assurance, achten wij van belang.

'Risk Management Principles for Electronic Banking'
Een ander voorbeeld van een richtlijn die van belang is voor de IT-audit, is de richtlijn 'Risk Management Principles for Electronic Banking' (mei 2001). Deze richtlijn is uitgebracht door de Electronic Banking Group, die zijn werkzaamheden uitvoert naast die van het Committee on Payment and Settlement Systems.
Op het moment van schrijven van deze tekst[3] was er nog geen definitieve richtlijn uitgebracht. In deze richtlijn zijn in drie hoofdcategorieën veertien principes uitgewerkt die het bankmanagement behulpzaam kunnen zijn bij het inzichtelijk krijgen, beheersen en controleren van de risico's die voortkomen uit e-bankieren. De hoofdcategorieën met daarbinnen de principes zijn:
* Board and management oversight:
  – Effective management oversight of e-banking activities;
  – Establishment of a comprehensive security control process;
  – Comprehensive due diligence and management oversight process of outsourcing relationships and other third-party dependencies;
* Security controls:
  – Authentication of e-banking customers;
  – Non-repudiation and accountability for e-banking transactions;
  – Appropriate measures to ensure segregation of duties;
  – Proper authorisation controls within e-banking systems, databases and applications;
  – Data integrity of banking transactions, records, and information;
  – Establishment of clear audit trails for e-banking transactions;
  – Confidentiality of key bank information;
* Legal and reputational risk management:
  – Appropriate disclosures for e-banking services;
  – Privacy of customer information;
  – Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services;
  – Incident response planning.

Aanvullend op het eerstgenoemde principe 'Effective management oversight of e-banking activities' wordt opgemerkt dat hieronder ook het proces van beleidsvorming valt. Uit de korte omschrijvingen van de principes valt op te maken dat deze principes goed kunnen dienen als uitgangspunt bij een door de IT-auditor uit te voeren IT-audit. Verder kunnen deze richtlijnen dienen voor de adviesfunctie van de IT-auditor. Zo is het mogelijk dat hij bij de Security control 'Non-repudiation and accountability for e-banking transactions' het advies geeft om een PKI-infrastructuur te implementeren.

Overige richtlijnen
In het jaar 2001 heeft de BIS tot medio november ruim vijftig publicaties laten verschijnen, die voor het overgrote deel door de BIS zélf of door het Basel Committee zijn uitgebracht. Het voert te ver om al deze publicaties in deze paragraaf te behandelen. Daarom is besloten

enkele voor de IT-audit relevante publicaties ter illustratie op te nemen, en wel:

* 'Internal audit in banks and the supervisor's relationship with auditors'
Een belangrijke aanleiding voor het verschijnen van deze richtlijn is te vinden in de publicatie van het nieuwe Basel Capital Accord. Dit akkoord bevat richtlijnen voor het toezicht op de minimumkapitaaleisen (capital adequacy framework), die zijn opgenomen in de 'Supervisory Review Pillar'. Door de definiëring van het taakgebied van de interne auditor en de toezichthouder wordt gestreefd naar een versterking van het toezicht op een financiële instelling. Deze richtlijn is voor de interne IT-auditor van belang omdat daarin onder meer aanwijzingen worden gegeven over:
– de reikwijdte van de audit, met name de verplicht uit te voeren risicoanalyse met betrekking tot de compliance, de betrouwbaarheid van financiële en managementinformatie, de continuïteit en betrouwbaarheid van de geautomatiseerde gegevensverwerking en het functioneren van stafafdelingen;
– de controletechnieken;
– de procedures.

Verder zijn er bepalingen opgenomen over de relatie met de toezichthouder, de externe auditor en het audit committee. Als laatste zijn er richtlijnen opgenomen over de uitbesteding van de interne controle.

* 'The relationship between banking supervisors and banks' external auditors'
In de zojuist genoemde publicatie over de relatie tussen de interne auditor en de toezichthouders is voornamelijk inhoudelijk ingegaan op de taakinhoud van de functie van de interne auditor en op basis daarvan wordt ingegaan op de relatie tussen beide. In de publicatie over de relatie tussen de externe auditor en de toezichthouders ligt de nadruk met name op de rolverdeling en relatie tussen beide, in plaats van op een inhoudelijke beschrijving van de taakinhoud van de externe auditor.

Committee on Payment and Settlement Systems
Het Committee on Payment and Settlement Systems (comité voor betalingsverkeer- en 'afwikkelings'systemen) richt zich op het bevorderen van de efficiency en stabiliteit van het nationale en internationale betalingsverkeer. Hiertoe vaardigt het richtlijnen uit met maatregelen ten aanzien van de opzet, het bestaan en de werking van de betalingsverkeersystemen.

Voor de beeldvorming wordt ook hier een aantal publicaties kort ter illustratie weergegeven:

* 'Recommendations for securities settlement systems'
In deze publicatie zijn negentien aanbevelingen opgenomen voor de opzet en inrichting van systemen voor settlement van effecten. Ter illustratie is een tweetal aanbevelingen opgenomen waaruit het belang van deze richtlijn voor de IT-auditor blijkt. Deze zijn:
– Operational Reliability
In de publicatie staat de volgende toevoeging vermeld: *'Sources of operational risk arising in the clearing and settlement process should be identified and minimized through the development of appropriate systems, controls and procedures. Systems should be reliable and secure and have adequate scalable capacity. Contingency plans and backup facilities should be established to allow for timely recovery of operations and completion of the settlement process.'*
In deze toevoeging staat een veelheid aan kwaliteitseisen die van belang zijn voor de IT-auditor.
– Access
Onder dit punt wordt aangegeven dat de diverse partijen toegang krijgen op basis van het 'need to know'-principe, de beperkingen die de wet- en regelgeving oplegt, etc.
De richtlijn geeft aanwijzingen op welke wijze aan deze aanbevelingen invulling kan worden gegeven, waarbij de IT ondersteunend is.

* 'Payment systems in Country XYZ; survey of electronic money developments'
Jaarlijks worden meerdere landen geselecteerd waarvan de ontwikkelingen in het nationale betalingsverkeer beschreven worden. De IT-auditor die zich specialiseert in het betalingsverkeer en de clearing- en settlementsystemen in een bepaald land kan bij zijn audits gebruikmaken van deze rapporten.

* 'Core Principles for Systematically Important Payment Systems'
In deze publicatie is een tiental principes uitgewerkt voor de zeer belangrijke betalingsverkeersystemen. Het belangrijkste principe voor de IT-auditor betreft:
'The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of a daily processing.'
In de toelichtende paragrafen wordt in detail ingegaan op de algemene aspecten en de kwaliteitsaspecten inzake beveiliging, betrouwbaarheid en continuïteit.

Committee on the Global Financial System
Deze commissie richt haar aandacht op het kortetermijntoezicht op de werking van het wereldwijde financiële systeem en de langetermijnanalyse van de werking van de financiële markten. Hiertoe vaardigt de commissie richtlijnen uit om de marktwerking te bevorderen. Omdat de door deze commissie uitgebrachte richtlijnen niet direct van invloed zijn op de IT-auditactiviteiten, zijn de werkzaamheden van deze commissie niet verder uitgewerkt.

Committee on Gold and Foreign Exchange
Dit comité heeft tot doel de goudvoorraden en forexmarkt (vreemdevalutamarkt) te monitoren en daarbij de langetermijn-probleempunten te onderkennen. Ten aanzien van langetermijn-probleempunten formuleert dit comité beleidsstandpunten en operationele processen om deze punten te adresseren. Omdat ook deze commissie richtlijnen uitbrengt die niet direct van invloed zijn op de IT-auditactiviteiten, zijn de werkzaamheden van deze commissie eveneens niet verder uitgewerkt.

Uitoefening toezicht

Zoals ook al uit de doelomschrijving van de BIS valt op te maken, vervullen de BIS en haar commissies meer een functie op het gebied van het ontwikkelen van richtlijnen en het onderzoeken en volgen van de ontwikkelingen binnen de financiële sector dan dat de bank een (actieve)

Drs. R.P. Schouten RE RA is als manager werkzaam bij KPMG Information Risk Management binnen de line of business Financial Services. Daarnaast is hij als manager werkzaam bij KPMG Accountants binnen de Financial Services Group. In beide functies heeft hij kennis en ervaring opgedaan binnen de bancaire, pensioen- en verzekeringsbranche alsmede assetmanagement. Hij heeft ervaring op de gebieden van quality assurance, projectreviews, pensioen- en verzekeringsprocesbeoordelingen, SAS 70-audits en auditsoftware-toepassingen. Verder is hij binnen IRM als national business development manager verantwoordelijk voor de productontwikkeling binnen Nederland.

toezichthouderrol vervult. Geconcludeerd kan worden dat de BIS op indirecte wijze het toezicht mede beïnvloedt door middel van het uitvaardigen van richtlijnen. Door de BIS worden probleemgebieden gesignaleerd, geadresseerd en vervolgens in de vorm van richtlijnen/beheerprincipes uitgewerkt. Het is uiteindelijk aan de nationale toezichthouders om de richtlijnen te onderschrijven en te incorporeren in hun eigen richtlijnen. Het zijn dan ook de nationale centrale banken die het directe toezicht uitoefenen op de invoering en naleving van deze richtlijnen. Voor de IT-auditor ligt er een taak om financiële instellingen in een vroegtijdig stadium te attenderen op het bestaan van belangrijke richtlijnen en de gevolgen van deze richtlijnen op de interne organisatie van informatievoorziening. Verder heeft hij de taak zijn (natuurlijke) adviesfunctie uit te oefenen, mede aan de hand van de richtlijnen.
Meerdere nieuwe BIS-richtlijnen, zoals bijvoorbeeld Bazel II, hebben een aanzienlijke impact op – soms nieuw – in te richten informatievoorzieningsprocessen, inclusief de daarbij te raadplegen bancaire (sub)systemen. Gezien het bovenstaande proces waarbij de nationale centrale banken de BIS-richtlijnen overnemen voor de eigen toezichthoudende functie, doen de interne en externe IT-auditors er verstandig aan om in een zo vroeg mogelijk stadium kennis te nemen van de in voorbereiding zijnde BIS-richtlijnen en hierop hun dienstverlening aan te passen dan wel in te richten. Op deze wijze zijn de interne en externe auditor in staat de eigen organisatie respectievelijk de klanten tijdig te wijzen op de impact van de richtlijnen en tevens een schatting te maken van de impact hiervan op de controleactiviteiten.

Samenvatting en nabeschouwing

Dat regelgeving een steeds belangrijker rol vervult bij het toezicht op de financiële sector mag evident zijn. In aanvulling hierop kan worden gesteld dat de beheersing van ICT een steeds belangrijker onderdeel gaat vormen in de bedrijfsvoering van de financiële instellingen en in de regelgeving van toezichthouders. In de ROB wordt in artikel 23 zelfs uitdrukkelijk aangegeven dat aandacht besteed moet worden aan de IT-aspecten. Ook in de regelgeving van de STE wordt expliciet aandacht geschonken aan de beheersing van IT.
De PVK daarentegen heeft geen specifieke voorschriften of richtlijnen uitgevaardigd ter beheersing van de IT. Aan de beheersing van IT in zijn algemeenheid is door de PVK tot op heden slechts beperkt aandacht besteed, met uitzondering van de problematiek inzake het millennium en de euro. Wel zijn recent voor pensioenfondsen, verzekeringsmaatschappijen en natura-uitvaartverzekeraars in concept Principes Interne Beheersing (PIB's) uitgebracht, welke de status van richtlijn hebben. Ook in deze PIB's echter wordt slechts in beperkte mate ingegaan op de beheersing van IT. De vraag doet zich derhalve voor of in de regelgeving van de PVK in voldoende mate aandacht wordt besteed aan de beheersing van IT en of hier vanuit de sector en vanuit de accountants meer behoefte aan bestaat. Des te meer omdat ook bij verzekeringsmaatschappijen en pensioenfondsen sprake is van een hoge mate van automatisering.

Ook internationaal bestaat er aandacht voor het opstellen van richtlijnen op velerlei gebied, zoals ook blijkt uit de gegeven toelichting op de BIS-regelgeving. Een groot verschil in de rol ten opzichte van die van de centrale banken wordt gevormd door het feit dat de richtlijnen van de BIS niet op een directe maar op een indirecte wijze een belangrijke rol vervullen in de door de (centrale) banken op te zetten normen. De reikwijdte van de normstelling door de BIS beperkt zich niet tot alleen het geven van richtlijnen voor het te voeren beleid, maar strekt zich ook uit tot normen voor de opzet en het beheer van de ICT. Met name deze laatste richtlijnen kunnen van belang zijn voor de door de IT-auditor uit te voeren audit- en advieswerkzaamheden. Voor de financiële instelling kan het van belang zijn om tijdig geïnformeerd te worden inzake bijvoorbeeld de impact van bepaalde richtlijnen op IT-systemen. Met betrekking tot BIS kan worden gesteld dat de keuze uiteindelijk aan de nationale toezichthouders is om de richtlijnen te onderschrijven en te incorporeren in hun eigen richtlijnen. Het zijn dan ook de nationale centrale banken die het directe toezicht uitoefenen op de invoering en naleving van deze richtlijnen.

Zowel DNB als STE verwijst naar 'sound practices' in haar regelgeving. DNB heeft de 'sound practices' echter in haar regelgeving niet uitdrukkelijk genoemd. Dit in tegenstelling tot de STE, die in de toelichting bij de Wijziging Nadere Regeling expliciet verwijst naar de Code voor Informatiebeveiliging, CobIT van ISACA en voor internettoepassingen naar de Handleiding ZekeRE Business van de NOREA. Opvallend is dat in de regelgeving van de PVK geen verwijzing is opgenomen naar bovengenoemde 'sound practices' en wel wordt verwezen naar 'sound practices' op het gebied van interne beheersingsmethoden zoals COSO. Dit is wellicht mede ingegeven door de (nog) beperkte mate van aandacht voor IT in de regelgeving.

Aan de betrokkenheid van de (externe) accountant en (externe) IT-auditor is in de regelgeving van zowel DNB als de STE aandacht besteed. Artikel 23 van de ROB geeft aan financiële instellingen de opdracht om aan de externe accountant een opdracht tot toetsing en beoordeling op hoofdlijnen van de toereikendheid van de organisatie-inrichting en het beheersingsmechanisme te verstrekken. In de controleaanpak van de STE wordt primair uitgegaan van de eigen verantwoordelijkheid van de instellingen en wordt waar mogelijk gesteund op de werkzaamheden van de interne accountantsdiensten en externe IT-auditors en accountants. Opvallend is dat in de toelichting van de Wijziging Nadere Regeling expliciet staat opgenomen dat beoordeling van de IT-specifieke onderdelen van de geautomatiseerde bedrijfsprocessen door gecertificeerde IT-auditors dient te worden uitgevoerd. Voor internetdiensten heeft de STE uitdrukkelijk aangegeven dat slechts toestemming wordt verleend indien door een onafhankelijke Register EDP-auditor onderzoek is gedaan naar de gehele keten van transactieverwerking, dus ongeacht welke automatiseringsorganisaties daarbij (waar ter wereld ook) zijn betrokken.

Door de wet- en regelgeving vanuit de PVK is de inzet van de IT-auditor niet verplicht gesteld. In de praktijk worden IT-auditors veelal wel ingeschakeld door accountants in het kader van de jaarrekeningcontrole. Hierbij wordt in de management letter aandacht besteed aan de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Echter, voor de jaarrekeningcontrole is niet beschreven welke werkzaamheden de accountant door de IT-auditor minimaal moet laten uitvoeren. Hierdoor kan onduidelijkheid bestaan omtrent scope en omvang van de door de IT-auditor uit te voeren werkzaamheden. De aandachtsgebieden voor de IT-audit zijn in de regelgeving van DNB en STE wel in voldoende mate benoemd om de IT-auditor voldoende houvast te geven bij het bepalen van de scope en omvang van zijn werkzaamheden. Aandacht wordt besteed aan het uitvoeren van risicoanalyses door instellingen, het opstellen van IT-beleid en informatiebeveiligingsbeleid en het opzetten van generieke en applicatieve maatregelen door instellingen ter beheersing van de IT- en de bedrijfsprocessen.

DNB heeft in haar regelgeving expliciet invulling gegeven aan te stellen eisen aan financiële instellingen in geval van het uitbesteden van (delen van) bedrijfsprocessen waaronder de automatisering. Bij de onder toezicht van de STE vallende instellingen blijkt dat de STE er in de praktijk wel van uitgaat dat de instelling verantwoordelijk is voor de gehele verwerkingsketen, dus inclusief de beveiliging en de verwerking door derde partijen. Derhalve dient de uitbestedende partij hiermee rekening te houden en na te gaan of de derde partij voldoet aan de STE-regelgeving. De PVK besteedt geen aandacht aan uitbesteding, hetgeen opvallend is omdat met name pensioenfondsen in hoge mate gebruikmaken van uitbesteding van vermogensbeheer en de administratie.

Concluderend kan worden gesteld dat elke toezichthouder eigen regelgeving heeft die in meerdere of mindere mate op onderdelen verschilt dan wel overeenkomsten vertoont. Ook qua diepgang in uitwerking bestaan er verschillen. De vraag rijst in hoeverre eventuele toekomstige ontwikkelingen ten aanzien van de hervorming van het toezichtsmodel aanpassing van de bestaande regelgeving met zich mee zullen brengen. Op sommige onderdelen zouden eventuele aanpassingen in de regelgeving ten aanzien van de beheersing van de IT een positieve bijdrage kunnen hebben voor de instellingen en ten aanzien van de uitvoering van de IT-auditwerkzaamheden.

De regelgeving van DNB en STE geeft de IT-auditor voldoende houvast bij het bepalen van zijn werkzaamheden.

Literatuur

[Beug00]
Mw. B. Beugelaar RE RA, *Internet-technologie, toezicht en de rol van IT-auditors bij financiële instellingen,* Compact 2000/1.

[DNB]
www.dnb.nl/handboeken/index.htm, Risk Analysis Manual DNB.

[DNB01]
De Nederlandsche Bank, *Regeling Organisatie en Beheersing*, definitieve versie d.d. 29 maart 2001.

[FinD01]
Het Financieele Dagblad, 'Zalm komt financiële sector tegemoet bij toezicht', 24 november 2001.

[Hoog01]
E. Hoogcarspel (KPMG), 'Ontwikkelingen Toezicht en Richtlijnen AO/IC', presentatie d.d. 11 december 2001.

[IOSC01]
International Organization of Securities Commissions, *Report on Securities Activity on the internet II*, June 2001 (www.iosco.org).

[KPMG01]
KPMG Financial Services Update 2001/2.

[Koni01]
E. Koning (DNB), NOREA/ISACA/VERA Congres 'Update on IT Assurance Services', presentatie d.d. 15 november 2001.

[NIVR01]
NIVRA, Audit Alert 11: *Werkzaamheden accountant in het kader van de Regeling Organisatie en Beheersing van De Nederlandsche Bank*, d.d. 2 augustus 2001.

[Osse01]
P.W. Osse RE RA, *Wijziging wet- en regelgeving bij financiële instellingen*, de EDP-Auditor, nummer 3, 2001.

[PVK]
Internetsite Pensioen- & Verzekeringskamer (www.pvk.nl).

[PVK01]
Concept Principes Interne Beheersing, Pensioen- & Verzekeringskamer, maart 2001.

[RFT00]
Raad van Financiële Toezichthouders, *Tussentijds bericht augustus 1999 – augustus 2000.*

[Teeu01]
W. Teeuwissen RA, 'Meldingsplicht, Informatieverstrekking door accountant en actuaris aan de PVK', presentatie d.d. 15 november 2001.