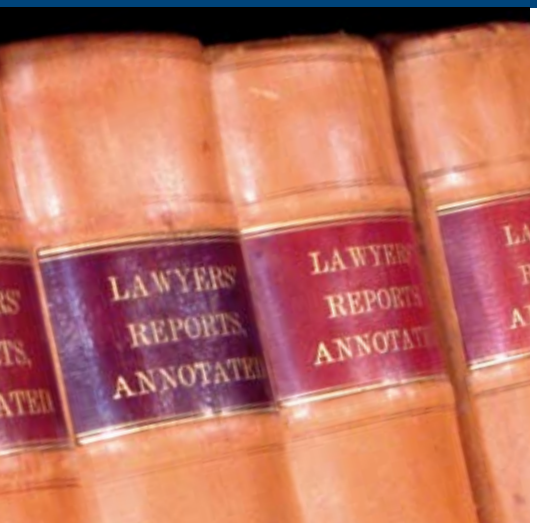


De inwerkingtreding van de Wft: wat verandert voor de IT-auditor?

Mw. ir. M.P. Jagt
is werkzaam als adviseur bij KPMG IT Advisory en heeft zowel adviesopdrachten als IT-audits uitgevoerd bij financiële instellingen, en wel in het bijzonder bij bancaire instellingen en pensioenfondsen.
jagt.marjanne@kpmg.nl

Ir. Marjanne Jagt

Met de komst van de Wft is de wetgeving voor de financiële markten doelgerichter, marktgerichter en transparanter geworden. Dit is bereikt door van acht verschillende wetten één wet te maken, voor zoveel mogelijk onderwerpen één algemene regel te maken en in de wet de taken van DNB en AFM te omschrijven en de samenwerking tussen beide toezichthouders te regelen.

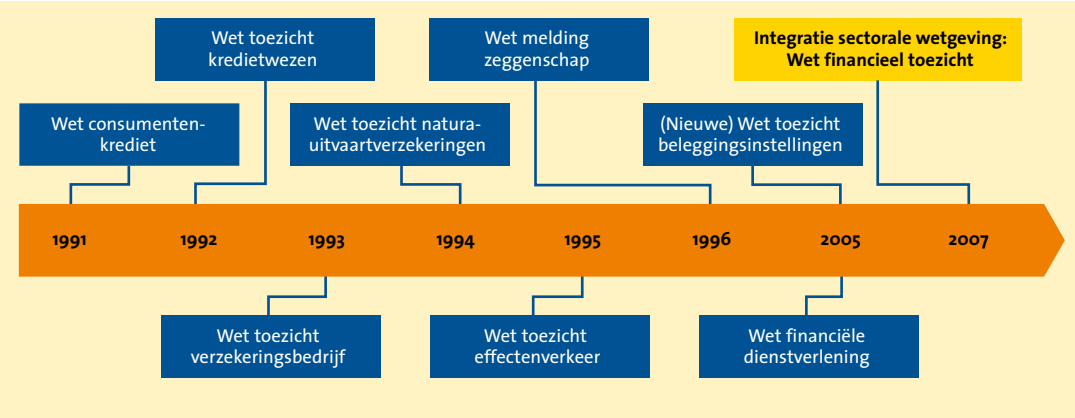
Inleiding

De Wet op het financieel toezicht (Wft) is op 1 januari 2007 in werking getreden. Deze wet regelt het toezicht op de financiële sector (met uitzondering van pensioenfondsen) in Nederland. Toezichtwet- en regelgeving heeft een lange geschiedenis. Oorspronkelijk was het toezicht op financiële ondernemingen per sector georganiseerd. Elke sector kende zijn eigen toezichtwet: een wet voor banken, een wet voor verzekeraars, een wet voor beleggingsinstellingen, enzovoort. De bepalingen van de verschillende wetten regelden veelal dezelfde onderwerpen. Voorbeelden zijn een vergunningplicht voor het aanbieden van bepaalde financiële diensten, regels ten aanzien van de bedrijfsvoering en betrouwbaarheidstoetsing van bestuurders. Op de financiële markten vond in toenemende mate een vervlechting plaats van ondernemingen en producten. Binnen de verschillende ondernemingen was steeds meer sprake van sectoroverstijgende activiteiten. Daarom werd in 2002 besloten tot een herziening van het toezicht op de financiële markten van het sectorale model naar een functioneel model. De Wft is het sluitstuk van deze herziening ([AFM06]).

In dit artikel staan de Wft en de impact hiervan op de werkzaamheden van de IT-auditor centraal. In de eerste paragraaf wordt beschreven wat er is veranderd met de komst van de Wft. In de volgende paragraaf wordt dieper ingegaan op raakvlakken van de Wft met de door een IT-auditor gehanteerde toetsingskaders. In de derde paragraaf wordt beschreven wat de gevolgen zijn voor de werkzaamheden van een IT-auditor. Het artikel sluit af met een conclusie.

Wat zijn de gevolgen van de invoering van de Wft?

De Wft vervangt acht toezichtwetten ([DNB08]), waaronder de Wet toezicht kredietwezen 1992 (Wtk), de Wet toezicht beleggingsinstellingen en de Wet financiële dienstverlening.



Figuur 1. **De weg naar de Wet op het financieel toezicht.**

Waar bancaire ondernemingen eerder moesten voldoen aan de Wet toezicht kredietwezen (Wtk) en de richtlijnen voor de uitvoering van toezicht, zoals de Regeling Organisatie en Beheersing (ROB), moeten banken vanaf 1 januari 2007 voldoen aan de wetgeving in de Wft en de daaraan gekoppelde regelgeving.

Het doel van de Wft is de regelgeving voor financiële markten doelgerichter en inzichtelijker te maken. Ook zijn de regels waaraan financiële instellingen moeten voldoen eenvoudiger gemaakt ([AFM06]). De Wft bestaat uit zes delen ([AFM06]):

- Algemeen;
- Markttoegang financiële ondernemingen;
- Prudentieel toezicht financiële ondernemingen;
- Gedragstoezicht financiële ondernemingen;
- Gedragstoezicht financiële markten; en
- Toezicht afwikkelsystemen.

Het deel Toezicht afwikkelsystemen zal later aan de wet worden toegevoegd.

De Wft regelt een aantal specifieke vormen van samenwerking tussen de AFM als gedragstoezichthouder en DNB als prudentieel toezichthouder. Hierdoor sluit de Wft – beter dan de oude wetgeving – aan bij de manier waarop er in Nederland toezicht wordt gehouden op financiële markten:

- De Nederlandsche Bank (DNB) voert het prudentieel toezicht, dat wil zeggen dat DNB de financiële stabiliteit (solvabiliteit en liquiditeit) en de betrouwbaarheid van financiële ondernemingen controleert.
- De Autoriteit Financiële Markten (AFM) voert het gedragstoezicht, wat inhoudt dat de AFM de marktwerking, de toetreding en het vertrouwen daarin controleert en bevordert.

De taakafbakening tussen DNB en AFM voorkomt niet dat beide toezichthouders actief zijn binnen dezelfde financiële sector. Mede om overlap in de uitoefening van de toezichttaken te voorkómen, is in de Wft zoveel mogelijk geregeld dat steeds één toezichthouder de bevoegdheid heeft om een besluit te nemen ([AFM06]).

Voor het gedragstoezicht zijn vooral de delen Algemeen, Markttoegang financiële ondernemingen, Gedragstoezicht financiële ondernemingen en Gedragstoezicht financiële markten relevant. Het deel Algemeen vormt de basis van het wettelijk kader. Hierin zijn de taken en bevoegdheden van de toezichthouders vastgelegd. In het deel Markttoegang financiële ondernemingen worden toegang tot de financiële markten en de vergunningplichtige activiteiten beschreven. Daarnaast zijn de voorwaarden vastgelegd waaronder een buitenlandse financiële onderneming toegang tot de Nederlandse financiële markten kan krijgen. Het deel Gedragstoezicht financiële ondernemingen bevat de regels waaraan financiële ondernemingen moeten voldoen bij het verlenen van hun diensten, zoals de regels voor het informeren van consumenten. Het deel Gedragstoezicht financiële markten bevat de regels waaraan spelers op de financiële markten zich te houden hebben, zoals de regels inzake marktmisbruik, emissies, openbare biedingen, melding van zeggenschap en kapitaalbelang in uitgevende instellingen ([AFM06]). De toezichthouder voor deze onderdelen is de AFM.

Voor prudentieel toezicht is het deel Prudentieel toezicht financiële ondernemingen relevant. Dit deel bevat de regels voor partijen op de financiële markten om aan hun financiële verplichtingen te voldoen. De toezichthouder voor dit deel is DNB.

De bepalingen zoals neergelegd in de Wft worden uitgewerkt in de onderliggende regelgeving. Deze bestaat uit twaalf besluiten of zogenaamde Algemene Maatregelen van Bestuur (AMvB's) ([MiFi07]). In figuur 2 is de wet- en regelgeving weergegeven en is te zien hoe de lagere regelgeving zich verhoudt tot de diverse delen van de wet.

Wft	Algemeen deel	Deel Markttoegang financiële ondernemingen	Deel Prudentieel toezicht financiële ondernemingen	Deel Gedragstoezicht financiële ondernemingen	Deel Gedragstoezicht financiële markten	Deel Toezicht afwikkel-systemen
AMvB's	Besluit bekostiging	Besluit markttoegang	Besluit prudentiële regels	Besluit gedragstoezicht financiële ondernemingen	Besluit melding zeggenschap en kapitaalbelang	
	Besluit definitie bepalingen	Besluit reikwijdte bepalingen	Besluit beleggers-compensatie en depositogarantie		Besluit marktmisbruik	
	Besluit boetes		Besluit prudentieel toezicht financiële groepen			

Figuur 2. **Indeling Wet op het financieel toezicht.**

Waarop en op wie is de Wft van toepassing?

De Wft geldt voor financiële ondernemingen en voor andere partijen die actief zijn op de financiële markten ([AFM06]). Een integrale wetgeving impliceert een integrale controle voor alle financiële instellingen. Toch wil het samenvoegen van alle regels nog niet zeggen dat de hele wet steeds van toepassing is op een specifieke financiële onderneming. Er wordt bijvoorbeeld in de wettekst onderscheid gemaakt tussen de wetgeving voor beleggingen en de wetgeving voor verzekeringen. Het is dus belangrijk om een goed overzicht te krijgen en te houden van de delen van de wetgeving die van toepassing zijn op de onderneming in kwestie. In de wet wordt aangegeven op welke product- en dienstcombinaties de Wft van toepassing is. Per productsoort gelden bovendien specifieke eisen. Een onderneming die verschillende producten aanbiedt moet dus aan verschillende eisen voldoen. De producten waarop de Wft van toepassing is, zijn ([SCFB06]):

- verzekeringen leven;
- verzekeringen schade;
- consumptief krediet;
- hypotheken;
- sparen en betalen (betaalrekeningen, spaarrekeningen);
- elektronisch geld;
- beleggen[1].

De nieuwe wet geldt onder meer voor:

- aanbieders van financiële producten:
  - verzekeraars,
  - banken;
- aanbieders van consumentenkrediet;
- aanbieders van beleggingsobjecten;
- adviseurs met betrekking tot financiële producten;
- bemiddelaars inzake financiële producten, inclusief bedrijven die het bemiddelen als nevenactiviteit hebben;
- herverzekeringsbemiddelaars;
- (onder)gevolmachtigde agenten.

Wat zijn de raakvlakken van de Wft met het controleraamwerk van een IT-auditor?

In deze paragraaf wordt beschreven welke onderdelen uit de Wft raakvlakken hebben met het vakgebied van een IT-auditor. Alvorens de attentiepunten uit de Wft voor de IT-auditor te behandelen, is het eerst van belang het controleraamwerk van de IT-auditor te beschrijven. Figuur 3 geeft een globaal overzicht van de onderwerpen die onderdeel uit kunnen maken van een IT-audit in het kader van de jaarrekeningcontrole waarbij de nadruk ligt op de betrouwbaarheid van de geautomatiseerde gegevensverwerking.

De Wft heeft invloed op verschillende niveaus van het bovenstaande IT-controleraamwerk. In dit artikel komen per niveau, zoals weergegeven in figuur 3, attentiepunten aan de orde. Deze attentiepunten zijn gerelateerd aan de relevante artikelen uit de Wft en de begeleidende Algemene Maatregelen van Bestuur (AMvB).

De Wft vormt in feite de raamwet waarbij AMvB's voor concrete invulling zorgen. In dit artikel wordt volstaan met een bondige en adequate beschrijving van hetgeen op hoofdlijnen in de wet of AMvB is vastgelegd. Wel wordt een verwijzing gemaakt naar artikelen en hoofdstukken waaruit het attentiepunt afkomstig is.

1) De Wft is beperkt van toepassing op beleggingen omdat er al een effectenwet is die veel regelt. Onder de Wft valt alleen het uitsluitend adviseren over beleggingen in effecten en het aanbieden van, adviseren over en bemiddelen in beleggingsobjecten.

Figuur 3. **IT-controleraamwerk.**

IT Governance #	Onderwerp (COSO)	Omschrijving	Ref. wet- en regelgeving
1	Control environment	De bedrijfsvoering van een financiële instelling omvat: a. een duidelijke en adequate organisatiestructuur; b. een duidelijke en adequate verdeling van taken, bevoegdheden en verantwoordelijkheden; c. een adequate vastlegging van rechten en verplichtingen; d. eenduidige rapportagelijnen.	AMvB 5:17, AMvB 8:31
2	Control environment	De betrouwbaarheid van personen die een integriteitgevoelige functie gaan bekleden, moet goed onderbouwd beoordeeld worden.	AMvB 5:13
3	Control environment	Een financiële onderneming is bij uitbesteding van werkzaamheden zelf verantwoordelijk voor het naleven van de daarop betrekking hebbende regels voor de derde partij.	Wft 3:18
4	Risk assessment	De onderneming voert gericht beleid op het beheersen van te lopen risico's. Risicobeheer moet op onafhankelijke wijze uitgevoerd worden en moet betrekking hebben op alle bedrijfsonderdelen.	AMvB 5:23-26
5	Risk assessment	Een financiële instelling zorgt voor systematische analyse van de bedrijfsrisico's. Daarnaast wordt beleid vertaald naar procedures en maatregelen, die (onafhankelijk) gecontroleerd en bijgesteld kunnen worden.	Wft art. 4.11, 4.14 en 4.15. AMvB 8:37
6	Information and Communication	De financiële onderneming of het bijkantoor beschikt over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking te waarborgen.	AMvB 5:20
7	Information and Communication	Een financiële onderneming voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot het op structurele basis uitbesteden van werkzaamheden.	AMvB 5:29
8	Information and Communication	De bedrijfsvoering van een financiële instelling omvat: e. een adequaat systeem van informatievoorziening en communicatie.	AMvB 5:17, AMvB 8:31
9	Monitoring	De onderneming beschikt over een onafhankelijke compliancefunctie die toezicht houdt op wettelijke en intern opgestelde regels.	AMvB 5:21, AMvB 8:31a/b, AMvB 8:38a
10	Monitoring	De financiële onderneming draagt zorg voor onafhankelijk toezicht op de uitvoering van het beleid en de procedures en maatregelen met betrekking tot de integere uitoefening van het bedrijf en beschikt over procedures die erin voorzien dat gesignaleerde tekortkomingen of gebreken worden gerapporteerd aan het management.	AMvB 5:10
11	Monitoring	Een financiële onderneming beschikt over toereikende procedures, maatregelen, deskundigheid en informatie om de uitvoering van de op structurele basis uitbestede werkzaamheden te kunnen beoordelen.	AMvB 5:30
12	Monitoring	Uitbesteding van werkzaamheden mag geen belemmering vormen voor het toezicht op naleving van het gedragstoezicht.	Wft 4:16, AMvB 5:27-32 , AMvB 8:37

Tabel 1. **Richtlijnen Wft voor IT-governance.**

IT General Controls			
#	Onderwerp	Omschrijving	Ref. wet- en regelgeving
1	Overall/ Operations	De bedrijfsvoering wordt door de externe accountant getoetst en beoordeeld op hoofdlijnen. De toetsing en beoordeling richt zich voornamelijk op de beheersing van die risico's die een materiële invloed kunnen hebben op de financiële prestaties, financiële positie en continuïteit van de financiële instelling. Belangrijk is dat de externe auditor aandacht besteedt aan IT-risico's.	AMvB 5:22
2	Access to programs and data / Operations	Bovenstaand beleid bestaat uit procedures en regels zoals: • autorisatieprocedures; • maatregelen voor noodsituaties.	AMvB 5:24
3	Operations	Een financiële onderneming beschikt over procedures en maatregelen met betrekking tot de omgang met en vastlegging van incidenten.	AMvB 5:12
4	Access to programs and data	Er is sprake van een duidelijke functiescheiding.	AMvB 5:18
5	Access to programs and data	Belangenverstrengeling wordt tegengegaan, daarvoor bestaan procedures en maatregelen.	Wft 4:14, AMvB 5:11, AMvB 8:18
6	Operations	De financiële onderneming of het bijkantoor beschikt over procedures en maatregelen om de voortdurende beschikbaarheid van geautomatiseerde gegevensverwerking te waarborgen.	AMvB 5:20

Tabel 2. **Richtlijnen Wft voor IT General Controls.**

De Wft schrijft vooral op het niveau van IT-governance een aantal belangrijke regels voor. In tabel 1 is een overzicht gegeven van de artikelen uit de Wft die raakvlakken hebben met het IT-controleraamwerk van de IT-auditor op het hoogste niveau (IT-governance).

Op de onderliggende niveaus (ITGC, application controls en IT dependent manual controls) schrijft de wet minder specifieke regels voor. In de tabellen 2 en 3 is weergegeven welke artikelen uit de Wft raakvlakken hebben met de overige niveaus uit het IT-controleraamwerk.

Centraal in de Wft staat een beheerste en integere bedrijfsvoering. Deze vormt tevens het vertrekpunt voor de externe toezichthouder om de naleving op de Wft te toetsen. Om dit te kunnen realiseren is risicomanagement belangrijk. Risicomanagement is dan ook verplicht gesteld in de Wft en is het vertrekpunt voor het te voeren beleid van een organisatie. Instellingen bepalen zelf op welke manier zij hun doelstellingen willen halen, zolang de keuzen maar zijn onderbouwd door middel van een risicoanalyse. Informatietechnologie is in dit keuzeproces een belangrijke ondersteunende factor, maar geen doel op zich. De Wft stimuleert zelfregulering.

DNB heeft ten behoeve van het uitoefenen van toezicht een methodologie opgesteld voor het uitvoeren van een risicoanalyse (FIRM). Deze methodologie wordt door DNB gehanteerd bij het uitvoeren van toezicht op de onder toezicht staande financiële instellingen, onder meer voor het opsporen van hoge inherente risico's en zwakke mitigerende beheersingsmaatregelen. Daarnaast wordt de methodologie door DNB gebruikt om de nadruk te leggen op die ondernemingen, of activiteiten binnen de organisatie, met een hoog risicoprofiel ([DNB]). De risicoanalyse en de daaruit voortvloeiende beoordelingscriteria kunnen ook door de instellingen gebruikt worden ter ondersteuning bij het uitvoeren van de risicoanalyse. Ook de IT-auditor kan gebruikmaken van deze risicoanalyse.

Uitbesteding is tevens een belangrijk onderwerp voor de IT-auditor. Voorheen was voor financiële instellingen de ROB van toepassing, waarin een tweetal paragrafen is opgenomen waaraan de uitbestedende partij moest voldoen. In het verleden is aan de IT-auditor gevraagd om in het kader van de jaarrekeningcontrole een uitspraak te doen in welke mate de instelling de ROB had nageleefd. De onderdelen van de ROB welke van toepassing zijn voor de IT-auditor betreffen ([Beug01]):

- paragraaf 2.5 Informatietechnologie (IT);
- paragraaf 2.6 Uitbesteding van (delen van) bedrijfsprocessen.

Doordat met de komst van de Wft de ROB is komen te vervallen, hebben veel IT-auditors moeite om de artikelen terug te vinden in de Wft. Tabel 4 geeft een overzicht van de artikelen uit de ROB met de verwijzing naar het corresponderende artikel in de Wft.

Application Controls			
#	Onderwerp	Omschrijving	Ref. wet- en regelgeving
1	Functiescheiding	De functiescheidingen binnen de geautomatiseerde gegevensverwerking sluiten aan bij de organisatiestructuur.	AMvB 5:20

Tabel 3. **Richtlijn Wft voor application controls.**

ROB	Omschrijving	Ref. naar Wft	Omschrijving
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.	AMvB 5:23.1, 4	1. Een financiële onderneming voert beleid gericht op het beheersen van de te lopen risico's. 4. De procedures en maatregelen worden vastgelegd en ter kennis gebracht van alle relevante bedrijfsonderdelen van de financiële onderneming.
Artikel 55	De instelling voert op systematische wijze een analyse van IT-risico's uit. De analyse wordt uitgevoerd zowel op instellingbrede basis als op het niveau van de onderscheiden bedrijfsonderdelen.	AMvB 5:23.5	De financiële onderneming voert op systematische wijze een onafhankelijk risicobeheer uit dat gericht is op het identificeren, meten en evalueren van de risico's waaraan de financiële onderneming is of kan worden blootgesteld. Het risicobeheer wordt zowel uitgevoerd ten aanzien van de financiële onderneming als geheel als ten aanzien van de onderscheiden bedrijfsonderdelen.
Artikel 56	De instelling draagt zorg voor de uitwerking en implementatie van 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.	AMvB 5:23.2 AMvB 5:24 AMvB 8:30.1d	Het beleid wordt vastgelegd in procedures en maatregelen ter beheersing van de te lopen risico's en geïntegreerd in de bedrijfsprocessen. Een financiële onderneming ziet er op systematische wijze op toe dat de procedures en maatregelen worden nageleefd en zorgt ervoor dat gesignaleerde tekortkomingen of gebreken worden opgeheven.
Artikel 57	De instelling draagt zorg voor specifieke maatregelen die een afdoende beveiliging van de informatie en de continuïteit van IT waarborgen. De rechtszekerheid en de privacy van de cliënten dienen bij gebruikmaking van IT-toepassingen in voldoende mate te zijn gewaarborgd.	Wft 4:91a2 Wft 5:30 AMvB 8:30.1c AMvB 8:31b	Regels en procedures voor een gezond beheer van de technische werking van het systeem en doeltreffende voorzorgsmaatregelen om met systeemstoringen verband houdende risico's te ondervangen.
Artikel 58	De instelling beschikt over helder geformuleerde beleidsuitgangspunten ter beheersing van de risico's die samenhangen met het uitbesteden van werkzaamheden. De beleidsuitgangspunten worden vastgelegd en gecommuniceerd aan alle relevante geledingen van de instelling.	AMvB 5:29	Een financiële onderneming voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot het op structurele basis uitbesteden van werkzaamheden.
Artikel 59	Ingeval de instelling onvoldoende waarborgen kan verkrijgen voor het handhaven van een beheerste en integere bedrijfsvoering, wordt niet tot uitbesteding van de desbetreffende bedrijfsprocessen overgegaan.	AMvB 5:28 AMvB 8:37 AMvB 8:38a	Een financiële onderneming gaat niet over tot het uitbesteden van werkzaamheden indien dat afbreuk doet aan de kwaliteit van haar onafhankelijke interne toetsing.
Artikel 60	De instelling draagt zorgt voor een systematische analyse van risico's die samenhangen met de uitbesteding van werkzaamheden. De analyse wordt uitgevoerd zowel op instellingsbrede basis als op het niveau van de onderscheiden bedrijfsonderdelen.	AMvB 5:23-26	De onderneming voert gericht beleid op het beheersen van te lopen risico's. Risicobeheer moet op onafhankelijke wijze uitgevoerd worden en moet betrekking hebben op alle bedrijfsonderdelen.
Artikel 61	De instelling werkt de beleidsuitgangspunten ter beheersing van uitbestedingsrisico's nader uit in organisatorische en administratieve procedures en maatregelen en integreert deze in de systemen en de dagelijkse werkzaamheden van alle relevante geledingen.	Wft 3:18.2b Wft 4:16 Wft 5:31 AMvB 5:29	Bij of krachtens algemene maatregel van bestuur: b. worden regels gesteld met betrekking tot de beheersing van risico's die verband houden met het uitbesteden van werkzaamheden door clearinginstellingen, kredietinstellingen en verzekeraars; en Een financiële instelling voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot het op structurele basis uitbesteden van werkzaamheden.
Artikel 62	De instelling legt de afspraken inzake uitbesteding met de externe dienstverlener/leverancier vast in een schriftelijke overeenkomst. Deze overeenkomst dient mede te voorzien in de bevoegdheid van de Bank om informatie in te winnen omtrent de uitbestede werkzaamheden bij de externe dienstverlener respectievelijk bij zijn externe accountant en desgewenst onderzoek te doen of te laten doen bij de externe dienstverlener/leverancier. Deze laatste verplichting geldt niet voor deelname aan een systeem als bedoeld in artikel 212a, onder b, van de Faillissementswet.	Wft 3:18.2c Wft 4:16 Wft 5:31 AMvB 5:31 AMvB 8:32.3 AMvB 8:38d	Bij of krachtens algemene maatregel van bestuur: c. worden regels gesteld met betrekking tot de door de financiële onderneming en de derde te sluiten overeenkomst met betrekking tot het uitbesteden van werkzaamheden. Een financiële onderneming legt de overeenkomst met de derde waaraan de werkzaamheden op structurele basis worden uitbesteed schriftelijk vast.
Artikel 63	Niet toegestaan is de uitbesteding van: de in artikel 22 van deze regeling bedoelde interne-auditfunctie aan een niet tot de groep behorende dienstverlener; de financiële administratie en het opmaken van de jaarrekening aan de controlerende externe accountant van de instelling, dan wel aan het kantoor waarmee de externe accountant is verbonden.	Niet expliciet opgenomen in Wft, echter wel: AMvB 5:27.2	2. Een financiële onderneming besteedt de taken en werkzaamheden van personen die het dagelijks beleid bepalen, daaronder mede verstaan het vaststellen van het beleid en het afleggen van verantwoording over het gevoerde beleid, niet uit.
Artikel 64	De instelling beschikt over procedures en maatregelen om toezicht te houden op de wijze waarop de externe dienstverlener/leverancier invulling geeft aan de uitbestede werkzaamheden.	Wft 3:18.1 Wft 3:18.3a Wft 4:16 Wft 5:31 AMvB 5:30 AMvB 8:38d	Indien een financiële onderneming werkzaamheden uitbesteedt aan een derde, draagt de financiële onderneming er zorg voor dat deze derde de ingevolge dit deel met betrekking tot die werkzaamheden op de uitbestedende financiële onderneming van toepassing zijnde regels naleeft. Een financiële onderneming beschikt over toereikende procedures, maatregelen, deskundigheid en informatie om de uitvoering van de op structurele basis uitbestede werkzaamheden te kunnen beoordelen.

Tabel 4. **Referentieoverzicht ROB naar Wft.**

Een aantal verschillen tussen de ROB en Wft is opmerkelijk. Door het verdwijnen van het verplichte karakter van de ROB lijkt het alsof een aantal specifieke eisen die door DNB aan uitbesteding werden gesteld, is komen te vervallen. De toezichthouder maakte in de ROB bijvoorbeeld geen verschil tussen interne en externe uitbesteding. De serviceorganisatie hoeft volgens DNB geen derde te zijn. In de definitie van DNB zit besloten dat het uitbesteden van een activiteit waarbij vertrouwelijke (kwetsbare) informatie de entiteit verlaat, door DNB wordt gezien als uitbesteding. Het gaat bij uitbesteding van (deel)processen steeds om risico's die een materiële invloed kunnen hebben op de financiële prestaties, de financiële positie, continuïteit of reputatie van de instelling. Voor deze beoordeling is een onderscheid tussen bancaire en ondersteunende processen als zodanig niet relevant. Tijdens het consultatieproces van de Wft is echter bewerkstelligd dat de Wft alleen van toepassing is op 'wezenlijke' (d.w.z. externe) uitbesteding. Dit zou een 'verlichting' ten opzichte van de huidige regelgeving zijn, aangezien de ROB externe en interne uitbesteding gelijkstelt qua eisen ([Bakko6]).

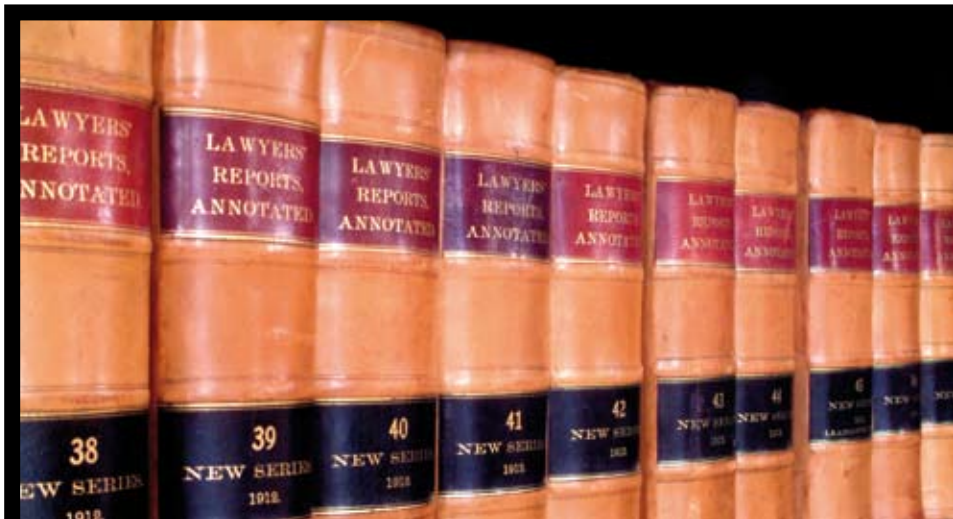
Een tweede belangrijk verschil ten opzichte van de ROB is dat minder nadruk wordt gelegd op een door de instelling op te stellen risicoanalyse bij een uitbesteding. In de Wft is geen *specifieke* eis opgenomen met betrekking tot het uitvoeren van een risicoanalyse in het kader van uitbesteding. Echter, zoals eerder genoemd, zijn in AMvB 5 wel algemene eisen gesteld aan het risicomanagementproces van de organisatie. Tevens zijn in AMvB 5 (Besluit prudentiële regels financiële ondernemingen; Bpr) en AMvB 8 (Besluit gedragstoezicht financiële ondernemingen; Bgfo) specifieke voorschriften over uitbesteding opgenomen. Als de uitvoering van operationele taken door een derde partij wordt overgenomen, moeten maatregelen worden getroffen die tot doel hebben het operationele risico te beperken. Omdat uitbesteding geen afbreuk mag doen aan de kwaliteit van de interne controle en geen belemmering mag vormen voor de werkzaamheden van toezichthouders (zowel AFM als DNB) blijft de onderneming verantwoordelijk voor alle diensten die worden uitbesteed aan derden. De eisen zullen derhalve moeten worden overgenomen in het uitbestedingscontract (service level agreement), bijvoorbeeld tijdige rapportage aan toezichthouders. De financiële instelling zal de uitvoering van de werkzaamheden moeten monitoren en controleren. Om aan deze eisen uit de Wft te voldoen kan uiteraard nog steeds goed gebruik worden gemaakt van de artikelen uit de ROB. De verwachting hiermee is dus dat er geen grote veranderingen zullen optreden. Indien een onderneming besluit over te gaan op uitbesteding van een activiteit zal dit op een beheerste wijze moeten worden uitgevoerd. Om dit proces te toetsen zal ook de (IT-)auditor nog steeds goed gebruik kunnen maken van de artikelen uit de ROB.

De impact van 'rule based'-toezicht naar 'principle based'-toezicht voor de IT-auditor

Huidige financiële ondernemingen en markten zijn te complex om 'alles' in detailregels te kunnen vastleggen. De invoering van de Wft brengt hier verandering in, doordat het toezicht in toenemende mate verandert van 'rule based'-toezicht naar 'principle based'-sturing. Terwijl 'rule based'-toezicht tot achter de komma voorschrijft welke maatregelen door een organisatie moeten worden getroffen, laat 'principle based'-toezicht meer vrijheid aan de organisatie zelf (zelfregulering). Inhoudelijk leidt de invoering van de Wft dus niet tot grote wijzigingen. Centraal staat een integere en beheerste bedrijfsvoering. Een organisatie krijgt hiermee meer vrijheid voor de inrichting van haar administratieve organisatie. Dit heeft tot gevolg dat 'principle based'-toezicht een minder normatief karakter kent. Echter, vanuit het externe toezicht zal wel worden gekeken wat het meest gangbaar is.

De rol van de IT-auditor bevindt zich in de overgangsfase van 'rule based'-audit naar 'principle based'-audit

De rol van de IT-auditor bevindt zich dus ook in de overgangsfase van 'rule based'-audit naar 'principle based'-audit. Van het signaleren van fouten op basis van strakke toetsingskaders naar het signaleren van risico's ter voorkoming van fouten. Daarbij doet zich een dilemma voor. Het blijkt lastig om risico's te inventariseren. Toezicht werkt alleen 'principle based' als de inbreng van de auditor als een signaal om van te leren wordt



opgevat. Van 'rule based' overstappen naar 'principle based' houdt ook in, dat je verder kijkt dan alleen de regels. De IT-auditor zal uitdrukkelijk de kwaliteit van de IT-processen en de prestaties waar een organisatie voor staat, in de audit moeten betrekken. Omdat de IT-auditor geen vast toetsingskader meer heeft, zal deze zich dus meer richten op het risicomanagement-proces. Op welke manier heeft de organisatie het risicomanage-mentproces ingericht? Hoe kan de organisatie aantoonbaar maken dat de onderneming haar risico's beheerst?

De gevolgen van deze veranderingen brengen met zich mee dat IT-auditors niet meer wegkomen met standaardvragenlijsten/normenkaders, maar steeds meer beleidsmatig en procedureel naar vraagstukken zullen kijken. De vraagstukken zijn hiermee steeds complexer geworden, omdat het beoordelen van beleid en procedures (vaak) onvoldoende zekerheid geeft. Het uitvoeren van een 'principle based'-audit zal ertoe moeten leiden dat op basis van een risicoanalyse de IT-auditor in de diepte onderzoek moet uitvoeren naar (de beheersing van) de IT-processen met een 'hoog risico'-classificatie en conclusies moet trekken op basis van detailbevindingen over wezenlijke problemen en oplossingen.

Conclusie

De conclusie is dat – hoewel een vrij uitgebreide lijst met voorwaarden is opgesteld – de Wft ten opzichte van de huidige regelgeving geen significante 'verzwaringen' en veranderingen met zich meebrengt voor de IT-auditor. Dit is natuurlijk ook niet vreemd gezien het feit dat de financiële instellingen altijd al aan het toezicht van DNB en AFM waren onderworpen door regels die in verschillende wetgevingen waren verankerd. Daarom kan in de praktijk nog steeds goed gebruik worden gemaakt van bijvoorbeeld sound practices van het British Standards Institute (BIS), de Regeling Organisatie en Beheersing en het toetsingskader business continuity planning (BCP).

De Wft is 'principle based' en dus niet 'rule based'. Er staan wel regels in maar het gaat bij instellingen om de handhaving van de principes. Principes als integer handelen, de principes die de instelling verwoord heeft in haar corporate values en de principes die ten grondslag liggen aan een solide bedrijfsvoering. Een dergelijke benadering vraagt zowel van de instelling als van de toezichthouder andersoortige inspanningen. Er zijn immers geen gedetailleerde regels waar het allemaal in staat. Het auditkader wordt gevormd door de wetgeving (Wet op het financieel toezicht) en reeds bewezen sound practices.

Literatuur

[AFM06] Autoriteit Financiële Markten, *Belangrijkste wijzigingen gedragstoezicht bij invoering Wft*, oktober 2006.

[Bakk06] Drs. R.W.A. Bakkers, *De rol van de compliancefunctie in het uitbestedingproces*, Tijdschrift voor compliance 2006-5.

[Beug01] B. Beugelaar en M. Ooms-Pieper, *Checklist IT aspecten Regeling Organisatie en Beheersing (ROB)*, Versie 1.0, 28 november 2001.

[DNB01] De Nederlandsche Bank, *Richtlijnen Organisatie en Beheersing*, www.dnb.nl.

[DNB05] De Nederlandsche Bank, *Handboek Financiële Instellingen Risicoanalyse Methode*, www.dnb.nl.

[DNB08] De Nederlandsche Bank, *Wet op het financieel toezicht*, www.dnb.nl/dnb/home/toezicht/nieuwe_toezichtwetgeving/wet_op_het_financieel_toezicht.

[MiFi07] Ministerie van Financiën, *Wet op het Financieel Toezicht, AMvB's en ministeriële regelingen*, november 2007.

- Besluit bekostiging financieel toezicht (AMvB 1)
- Besluit definitiebepalingen (AMvB 2)
- Besluit boetes Wft (AMvB 3)
- Besluit markttoegang financiële ondernemingen (AMvB 4)
- Besluit reikwijdte bepalingen (AMvB 4a)
- Besluit prudentiële regels Wft (AMvB 5)
- Besluit bijzondere prudentiële maatregelen, beleggerscompensatie en depositogarantie (AMvB 6)
- Besluit prudentieel toezicht financiële groepen (AMvB 7)
- Besluit Gedragstoezicht financiële ondernemingen (AMvB 8)
- Besluit melding zeggenschap en kapitaalbelang in uitgevende instellingen (AMvB 9)
- Besluit marktmisbruik Wft (AMvB 10).

[SCFB06] StudieCentrum Financiële Branche, *Invoering Wft: grote gevolgen voor financieel adviseurs*, 2006 (http://www.scfb.nl/artikel/110.htm).