Uitbesteding bij financiële ondernemingen

Wet- & regelgeving en de IT-auditor (Deel 1 - Wft)

Jeroen van Puijenbroek

Het uitbesteden van taken en activiteiten door financiële ondernemingen is tegenwoordig aan de orde van de dag. De voornaamste redenen? Kostenreductie en verhoging van de kwaliteit. Aan uitbesteding kleven echter ook risico's. Daarom worden op grond van wet- en regelgeving eisen gesteld aan uitbesteding bij financiële ondernemingen

Auteur

Mr. drs. J.P.M. (Jeroen) van Puijenbroek RE werkt als senior auditor bij de Audit Rabobank Groep van Rabobank Nederland. Van Puijenbroek is voornamelijk werkzaam op het gebied van het ontwikkelen en (mede)uitvoeren van compliance audits. De auteur heeft het artikel op persoonlijke titel geschreven.

Het feit dat een financiële onderneming zijn back office uitbesteedt aan een andere partij haalt de kranten vaak niet meer. Enkele voorbeelden uit het afgelopen decennium. AEGON behoort in Nederland tot de voorlopers op het gebied van uitbesteding. Het bedrijf begon in 1998 met het uitbesteden van applicaties bij Pink Elephant en in 2000 volgden de infrastructuur en de ondersteuning van de werkplekken.[1] ABN AMRO besteedde in 2002 een groot deel van zijn wereldwijde IT-activiteiten in de Wholesale divisie uit aan EDS.[2] De Rabobank heeft eind 2006 gekozen voor de uitbesteding van een deel van haar systeemontwikkelingsproces aan Ordina en Cognizant Technology Solutions.
Sinds enkele jaren moeten ook bedrijfsprocessen er aan geloven. Zo besteedde de ABN-AMRO in 2004 haar 'asset & fund' management uit aan een Amerikaanse bank; het portfoliomanagement (de beslissing over wat moet worden gekocht en verkocht) werd als 'core' beschouwd, maar alles wat daarna gebeurt (het daadwerkelijk kopen of verkopen van aandelen, obligaties, opties, etc.) kan worden uitbesteed aan een bank die het beter en/of goedkoper kan.[3]

Waarom worden zoveel bedrijfsactiviteiten tegenwoordig overgedragen aan gespecialiseerde derden (serviceorganisaties), die deze activiteiten vervolgens terugleveren als diensten? Een belangrijke reden om activiteiten of processen uit te besteden is kostenreductie. Deze wordt bereikt doordat de serviceorganisatie schaalvoordelen kan behalen door deze activiteiten voor meerdere partijen uit te voeren. Dit resulteert in een lagere kostprijs. Behalve de kostenreductie is de verhoging van de kwaliteit een belangrijke drijfveer. Dit kan worden gerealiseerd door betere IT, beter ingerichte processen en op dat gebied toegewijd en deskundig management. Ook vastlegging van afspraken in een SLA (Service Level Agreement) kan leiden tot een verbetering (en vooral een betere voorspelbaarheid) van de kwaliteit.[4] Naast de voordelen zijn aan uitbesteding ook nadelen (lees: risico's) verbonden. Hierbij kan worden gedacht aan:

- een serviceorganisatie die niet in staat is de service te leveren volgens de in de SLA vastgestelde normen;
- de afhankelijkheid van een serviceorganisatie terwijl de financiële onderneming juist maximale flexibiliteit nodig heeft;
- de mogelijkheid dat de strategische focus van de serviceorganisatie verandert;
- de mogelijkheid dat uitbesteding heeft plaatsgevonden

naar een serviceorganisatie die in een later stadium word gekocht door een concurrent;
- de kans op insolventie of faillissement van de serviceorganisatie;
- het in rekening brengen van hoge kosten door de leverancier voor het leveren van extra service als gevolg van slecht gedefinieerde contractuele voorwaarden voor de geleverde diensten.

Wanneer een onderneming uitbesteedt, dient zij naast bovenstaande risico's (waarop in deze publicatie overigens niet verder wordt ingegaan) ook rekening te houden met diverse (sectorale) wet- en regelgeving. In dit artikel geven we aan de hand van de compliance chart een overzicht van de relevante regelingen voor een financiële onderneming. Op een van deze wetten, namelijk de Wft, zal vervolgens nader worden ingegaan. Naast een korte uitleg over de uitgangspunten en de structuur van de Wft zal ook per fase van het uitbestedingproces worden aangegeven waar de IT-auditor rekening mee moet houden respectievelijk wat zijn rol kan zijn. Voordat wordt ingegaan op regelgeving en IT-auditor zal eerst worden ingegaan op de fasen van het uitbestedingproces.

Fasen uitbestedingproces

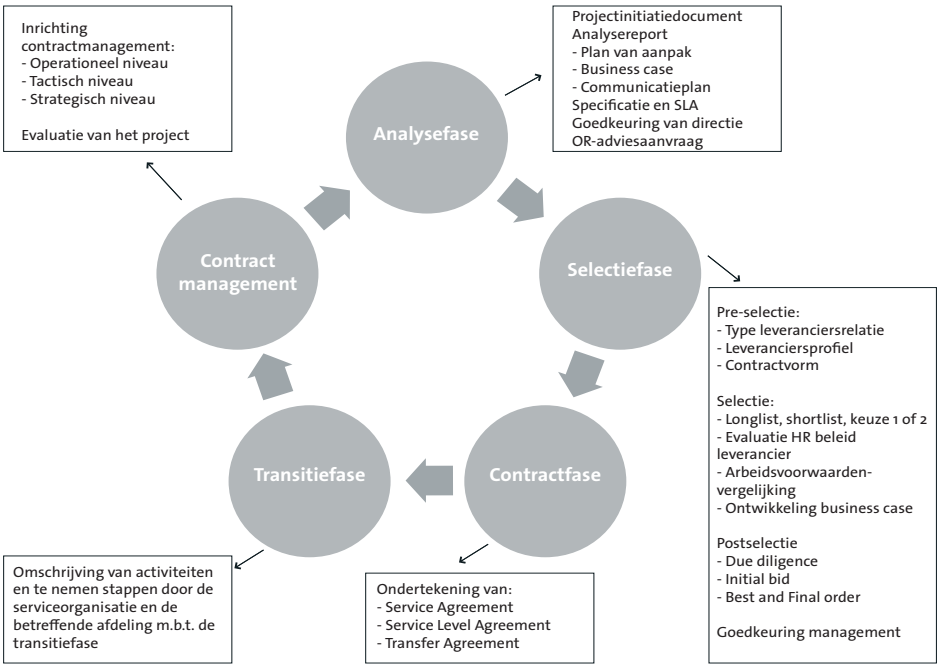
Het uitbestedingproces bestaat grofweg uit vijf fasen[5], te weten:
1. Analysefase
2. Selectiefase
3. Contractfase
4. Transitiefase
5. Contractmanagement

In figuur 1 is dit grafisch weergegeven.

Ad. 1) Analysefase
Het proces start met de analysefase. In deze fase analyseert het projectteam de activiteit(en) die in aanmerking komen voor uitbesteding, met als resultaat een uitvoerige business case en een concreet plan van aanpak. Vervolgens wordt het analyserapport – het plan van aanpak met de business case – ter beoordeling voorgelegd aan de betreffende directie, bijvoorbeeld de afdeling Automatisering. Belangrijkste op te leveren producten ('deliverables') en/of activiteiten in deze fase zijn projectinitiatiedocument, analyserapport (plan van aanpak, business case, communicatieplan), specificatie & concept SLA goedkeuring directie en -adviesaanvraag Ondernemingsraad.

Ad. 2) Selectiefase
Bij goedkeuring kan het projectteam starten met de volgende fase, de selectiefase. De kwalificaties waaraan verschillende leveranciers moeten voldoen en de mate waarin zij hieraan voldoen worden in deze fase naast elkaar gezet. Belangrijkste op te leveren producten en/of activiteiten in deze fase zijn preselectie (type leveranciersrelatie, leveranciersprofiel, contractvorm), selectie (longlist, shortlist, keuze 1 of 2, evaluatie HR-beleid leverancier, arbeidsvoorwaardenvergelijking, ontwikkeling business case), postselectie (due diligence, initial bid, best and final order) en goedkeuring management.

Ad. 3) Contractfase
Het onderhandelingsproces wordt in de selectiefase al in gang



Figuur 1: Fasen uitbestedingproces

gezet en loopt door in de contractfase. In de contractfase vinden de laatste onderhandelingen plaats en worden de gemaakte afspraken in een contract vastgelegd. De op te leveren producten in deze fase zijn de ondertekende Service Agreement, Service Level Agreement en Transfer Agreement.

Ad. 4) Transitiefase
Na het tekenen van het contract volgt de transitiefase, de feitelijke transitie van mensen, processen, services, technologieën en assets. De belangrijkste op te leveren producten in deze fase zijn een omschrijving van activiteiten en te nemen stappen door de leverancier en de betreffende directie.

Ad. 5) Contractmanagement
De laatste fase, wellicht de belangrijkste fase van het uitbestedingproces, betreft het managen van het contract. De belangrijkste op te leveren producten en/of activiteiten zijn inrichting contract management op operationeel, tactisch en strategisch niveau en de evaluatie van het project.

Compliance chart
Het is van belang om direct aan het begin van een uitbestedingproject inzicht te hebben welke wet- en regelgeving van toepassing is. Dit geldt zeker bij financiële ondernemingen, die te maken hebben met toezichthouders als De Nederlandse Bank (DNB) en de Stichting Autoriteit Financiële Markten (AFM). Welke eisen worden door hen gesteld aan uitbesteding? Zijn er activiteiten die niet mogen worden uitbesteed? Et cetera.
Het kost immers veel minder tijd en dus ook minder geld als vooraf de kaders zijn vastgesteld die inzichtelijk maken waaraan moet worden voldaan dan wanneer achteraf allerlei zaken moeten worden aangepast. Niet dat die wetten en regels allerlei exotische eisen stellen aan uitbesteding. Aan het overgrote deel van de onderwerpen die bij wet of regelgeving is geregeld, zou een onderneming op grond van goed ondernemerschap toch al aandacht (moeten) hebben besteed. Het management van een onderneming wil immers zelf toch ook weten of ze nog steeds 'in control' is na uitbesteding van de activiteit en niet alleen omdat de toezichthouders dat graag willen weten.

De compliance chart is een overzicht van alle van toepassing zijnde regelgeving. Per uitbestedingproject dient een overzicht van de volgende typen regelgeving te worden opgesteld[6]:
- Externe regelgeving betreffende uitbesteding.
- Interne regels/richtlijnen/beleidslijnen (interne regelingen) betreffende uitbesteding.
- Specifieke regelgeving die van toepassing is op de uit te besteden dienst.

Naast de meer generieke wetten (intellectueel eigendomsrecht, arbeidsrecht, fiscaal recht en mededingingsrecht) dient bij externe regelgeving ook aandacht te worden besteed aan specifieke wet- en regelgeving op grond van de sector waarin de organisatie opereert, de aard van de uit te besteden activiteit, de aard van de onderneming, of de uitbesteding binnen of buiten Europa plaatsvindt, et cetera. Voor financiële ondernemingen is bij uitbesteding onder meer de volgende wet- en regelgeving relevant:
- Wet financieel toezicht (Wft).
- Markets in Financial Instruments Directive (MiFID).
- Wet bescherming persoonsgegevens (Wbp).

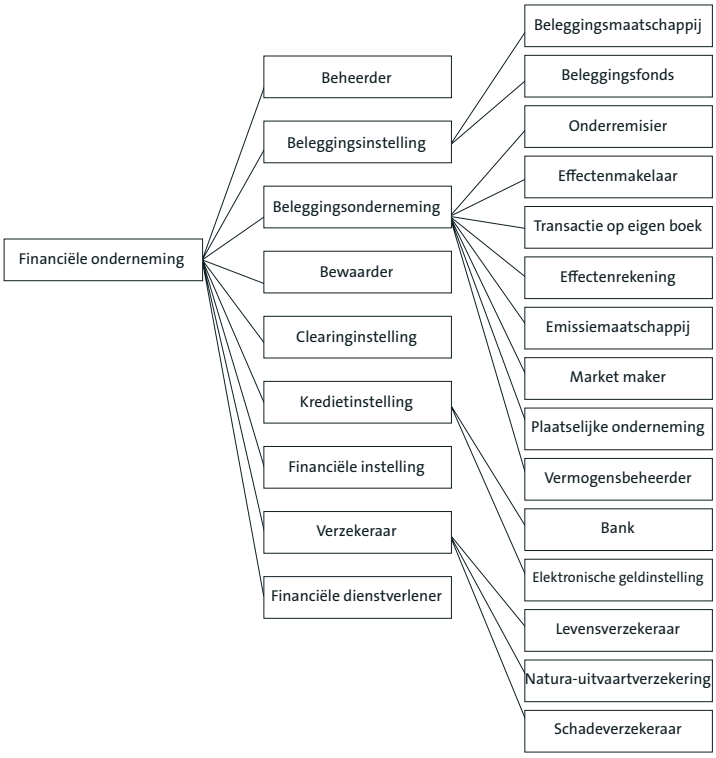
Bij specifieke regelgeving die van toepassing is op de uit te besteden dienst moet bijvoorbeeld worden gedacht aan de Voorwaarden en Normen Nationale Hypotheekgarantie in geval van het uitbesteden van (delen van) de hypotheekverstrekking. Deze en andere specifieke regelgeving blijft in deze publicatie buiten beschouwing.

Het opstellen van de compliance chart zal veelal een taak zijn van de compliancefunctionaris. Bij een audit naar het uitbestedingproces kan de IT-auditor de totstandkoming van de chart en de betrokkenheid van de compliancefunctionaris beoordelen. Welke functionarissen waren betrokken bij het opstellen van de chart, heeft er een review op plaats gevonden, wordt onderscheid gemaakt naar type regelgeving (extern, intern en specifiek), op welke wijze is geborgd dat de financiële instelling en de dienstverlener aan de opgenomen regelgeving (gaan) voldoen, et cetera.

In de rest van deze publicatie zal nader worden ingegaan op de Wft in relatie tot uitbesteding. In een eerder artikel in dit tijdschrift zijn Bolderhey en IJpeij al ingegaan op de gevolgen van de per 1 november 2007 van kracht geworden MiFID.[7] In een van de volgende uitgaven van de IT Auditor zal de Wbp in relatie tot uitbesteding door financiële ondernemingen aan bod komen.

Wet financieel toezicht
In dit deel gaan we in op de achtergrond van de Wft, de structuur van de wet en de belangrijkste uitgangspunten bij het opstellen ervan. Daarna gaan we nader in op die delen van de Wft waarin eisen zijn opgenomen over uitbesteding.

Achtergrond
Op 1 januari 2007 is de Wft in werking getreden. De Wft is het resultaat van de hervorming van de financiële toezichtwetgeving. Met de inwerkingtreding heeft een ´kanteling van toezicht´ plaatsgevonden, van een sectoraal model naar een functioneel model. Deze hervorming is mede ingegeven door een aantal ontwikkelingen binnen de financiële marktsector, zoals de toenemende internationalisering van financiele markten en de vervlechting van financiële producten en diensten, het ontstaan van internationaal en sectoroverstijgend actieve ondernemingen, en conglomeraatvorming. Het oude sectorale model, waarin per categorie financiële ondernemingen een aparte toezichtwet bestond, voldeed hierdoor niet meer. In de Wft zijn maar liefst zeven oude toezichtwetten opgenomen[i]. Onder de Wft is de term 'financiële onderneming' dan ook een heel ruim begrip. In figuur



Figuur 2: Overzicht van financiële ondernemingen (bron: EYe on Finance – Special Wet op het financieel toezicht[8])

2 is dit schematisch weergegeven.

Structuur: Prudentieel en gedragstoezicht

Het financieel toezicht is in de Wft ingedeeld op basis van twee pijlers, te weten:

- *Prudentieel toezicht* op financiële ondernemingen, dat wordt uitgevoerd door DNB. Prudentieel toezicht is gericht op de bedrijfseconomische prestaties van individuele financiële ondernemingen. Het prudentieel toezicht van DNB bestaat uit het toezicht op de solvabiliteitspositie, de liquiditeitspositie en op operationeel risico.
- *Gedragstoezicht* op financiële markten, dat is opgedragen aan AFM. Gedragstoezicht is gericht op de integriteit van een financiële onderneming en haar medewerkers. Belangrijke onderdelen van het gedragstoezicht zijn bijvoorbeeld regels met betrekking tot Chinese Walls[ii], koersgevoelige informatie/privé-beleggingtransacties en gedragsregels voor individuele medewerkers.

In figuur 3 is de structuur van de Wft weergegeven. De delen waarin artikelen over uitbesteding zijn opgenomen zijn donker weergegeven. Hierin ziet men de twee pijlers van prudentieel toezicht en gedragstoezicht ook terugkomen.

Uitgangspunt: 'Principle based' in plaats van 'rule based' toezicht

Een van de belangrijke uitgangspunten van de Wft is dat sprake is van *principle based* toezicht in plaats van *rule based* toezicht. Wat houden deze begrippen eigenlijk in en wat betekent dit voor de financiële onderneming?

Bij *rule based* toezicht streeft de wetgever ernaar de regels waaraan moet worden voldaan zo nauwkeurig mogelijk te omschrijven. Daarbij wordt dus uitwerking gegeven aan de achterliggende gedachte van de regels, met als resultaat zoveel mogelijk helderheid voor de gebruiker. Het risico hiervan is dat in sommige gevallen de regels worden uitgewerkt op een wijze die in de praktijk niet de meest gunstige is voor de onderneming. Dat risico wordt bij *rule based* toezicht door de wetgever voor lief genomen.

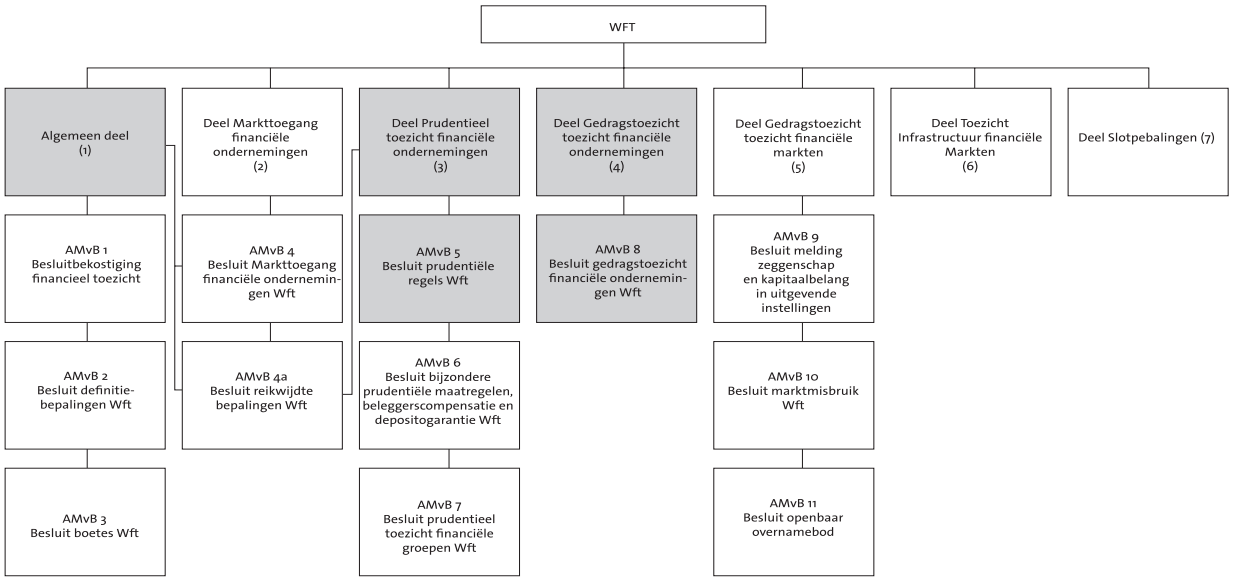
Bij *principle based* toezicht volstaat de wetgever met een open norm en laat hij het aan de ondernemingen over om te bepalen op welke wijze zij eraan voldoen. Dit lijkt soft, aldus voormalig minister Zalm in een toespraak op het Wft-seminar 2006[9], maar dient om te voorkomen dat gebruik wordt gemaakt van juridische redeneringen of constructies die volgens de letter van de wet kloppen, maar tegen de geest van de wet zijn. Denk bijvoorbeeld aan Enron: heeft deze onderneming gehandeld in strijd met de letter of met de geest van de geldende Amerikaanse wetgeving?

Bij *principle based* toezicht worden de algemene normen in een wet minder strikt uitgewerkt in lagere regelgeving dan bij *rule based* toezicht en wordt bij de uitvoering van het toezicht vooral gekeken of aan de doelstellingen van een wettelijke norm wordt voldaan en niet zozeer naar de wijze waarop dat exact gebeurt. De open norm geeft alleen het doel weer; *hoe* de dienstverlener het doel wil bereiken is aan hem en hij zal zelf de normen moeten gaan interpreteren. Niet wordt voorgeschreven hoe de dienstverlener zijn bedrijfsvoering dient in te richten om aan te tonen dat hij aan de wetgeving voldoet; de open norm is dus tevens vormvrij. Dit geeft partijen de meeste vrijheid om een bij hun situatie passende wijze van naleving te waarborgen. De onderneming kan hierdoor dicht bij haar eigen situatie blijven, wat lagere kosten betekent. De open norm leidt tot grotere eigen verantwoordelijkheid, het dwingt tot nadenken in plaats van slaafse navolging, maar kan ook tot grotere onzekerheid leiden (gaat DNB akkoord? gaat AFM akkoord?). AFM stelt zelf: 'De open normen in wet- en regelgeving, alsmede de benodigde interpretatie van nieuwe regels, maakt de uitvoerbaarheid en het toezicht complexer'. [10]

Door de harmonisering van de sectorale regelgeving en het uitgangspunt van open normen is de wet compacter maar ook een stuk abstracter geworden. Dit heeft geleid tot wat wel eens het 'zwarte gat' van de Wft wordt genoemd, de lezer ziet het niet maar het heeft wel veel impact. De abstractere formulering van de wet 'triggert' minder snel tot de vraag 'heeft het in onze onderneming invloed?'.

Wft en uitbesteding

In deze paragraaf wordt uiteengezet wat de Wft onder uitbesteding verstaat en wordt aangegeven in welke delen van de wet er eisen worden gesteld aan uitbesteding.



Figuur 3: Structuur Wft en uitbesteding

Deel 1 Wft (Algemeen deel)

In het algemene deel van de Wft is in artikel 1 lid 1 de definitie van uitbesteden opgenomen.[11] Deze luidt:

Uitbesteden: het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:

a. die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of
b. die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan.[12]

Van uitbesteden is volgens de toelichting op de definitie sprake indien 'werkzaamheden die normaal worden verricht binnen de financiële onderneming worden verricht door derden, waaronder ook wordt verstaan andere ondernemingen binnen de groep waartoe de financiële onderneming behoort. Te denken valt aan het uitbesteden van de automatisering. Het laten leveren van gestandaardiseerde producten als marktinformatie of kantoorinventaris (inkoop) door andere ondernemingen binnen de groep waartoe de financiele onderneming behoort of door derden valt niet onder het uitbesteden van werkzaamheden'.[13]

De inkoop van goederen of advieswerkzaamheden ten behoeve van die bedrijfsprocessen vallen evenmin onder uitbesteding. Het moet wel gaan om (delen van) wezenlijke bedrijfsprocessen die worden uitbesteed. In dat verband is een juridische dienst voor een financiële onderneming over het algemeen niet wezenlijk. Dit kan echter anders zijn, bijvoorbeeld in het geval van een rechtsbijstandverzekeraar die niet de kosten van rechtsbijstand vergoedt, maar de rechtsbijstand in natura aanbiedt.[14] Met de term '*wezenlijk*' in de definitie van uitbesteden wordt tot uitdrukking gebracht dat niet elk bedrijfsproces voor het toezicht van DNB of AFM van belang is.

Onder het uitbesteden van werkzaamheden valt evenmin de inhuur van externen, zoals uitzendkrachten, inleenkrachten, gedetacheerde ICT-ers, et cetera. Deze personen zijn immers werkzaam binnen de eigen organisatie en vallen direct onder interne leidinggevenden.

Deel 3 en 4 Wft

Door de invoering van de Wft zijn de uitbestedingregels geharmoniseerd voor banken, verzekeraars, beleggingsinstellingen, beleggingsondernemingen en clearinginstellingen. De wettelijke grondslag voor het stellen van grenzen en voorwaarden aan (toelaatbare) uitbesteding is opgenomen in artikel 3:18 Wft (deel 3) voor banken en andere instellingen die onder prudentieel toezicht vallen en in artikel 4:16 Wft (deel 4) voor ondernemingen die onder gedragstoezicht vallen. Er is een duaal toezicht op uitbesteden van werkzaamheden. DNB houdt toezicht op uitbesteding voor zover het gaat om algemene aspecten, integriteitaspecten en het invloed kan hebben op de soliditeit. AFM houdt toezicht op uitbesteding voor zover het gaat om transparante financiële marktprocessen, de zuivere verhouding tussen marktpartijen en zorgvuldige behandeling van klanten.

In het Besluit prudentiële regels Wft (Bpr) en in het Besluit gedragstoezicht financiële ondernemingen Wft (BGfo) zijn de nadere voorschriften opgenomen. De tot 1 januari 2007 bestaande toezichthouderregels betreffende uitbesteding zijn ingetrokken zoals de Regeling Organisatie en Beheersing (ROB), de Regeling Uitbesteding Verzekeraars (RUV), de Nadere regeling gedragstoezicht effectenverkeer 2002 (NRge2002). De artikelen in de hierboven genoemde besluiten zijn over het algemeen *principle based*.

Wft en de IT-auditor

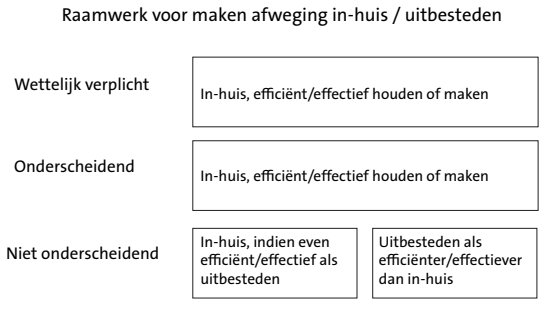
In tegenstelling tot *rule based* toezicht, waarbij de specifieke eisen uit de wet- en regelgeving een concrete basis vormen

voor het op te stellen normenkader, moet de auditor bij *principle based* toezicht deze normen zelf invullen en interpreteren. Welke handvatten heeft de IT-auditor voor het invullen en interpreteren van de open normen van de Wft bij een audit naar de rechtmatigheid van de uitbesteding van de werkzaamheden bij een financiële onderneming? Naast de Nota van toelichting op het besluit kunnen hierbij ook de oude toezichtregels (ROB, RUV, NGre2002, Interpretatie AFM uitbesteding door effecteninstelling, et cetera) als handreiking dienen bij het concretiseren. Voor de interpretatie van een norm kan de auditor ook nog de hulp inroepen van DNB of AFM. AFM heeft bijvoorbeeld in het beleidsplan 2007-2009 aangegeven dat ze in gevallen waar de wetgeving bewust ruimte laat voor interpretatie een duidelijk oriëntatiepunt wil vormen.[15] Om dit soort complianceaudits goed te kunnen uitvoeren dient de IT-auditor, dan wel het auditteam, te beschikken over voldoende kennis van de Wft en de onderliggende besluiten en regelingen. Indien deze kennis niet aanwezig is, kan ondersteuning worden gegeven door een juridisch adviseur.

Hieronder is een aantal open normen van de Wft voor de fasen van het uitbestedingproces geconcretiseerd.

Analysefase
De normen uit de Wft hebben betrekking op de aard van de uit te besteden werkzaamheden, of beter gezegd het verbod om bepaalde werkzaamheden uit te besteden, en het uitvoeren van een risicoanalyse

Verbod uitbesteden
Bij de afweging tussen uitbesteden en de activiteit in huis houden/(terug)nemen speelt naast de eerdergenoemde voordelen en nadelen, het onderscheidend vermogen van de betreffende activiteit en de mate van efficiëntie en effectiviteit van de uitbestedende onderneming ook nog ander aspect een rol. Op basis van de Bpr en BGfo mogen bepaalde activiteiten niet worden uitbesteed. Zo mogen in het algemeen werkzaamheden niet worden uitbesteed indien die uitbesteding een belemmering kan vormen voor het adequaat toezicht door DNB of AFM. Meer specifiek, de taken en werkzaamheden van personen die het dagelijks beleid bepalen mogen niet worden uitbesteed en de interne auditafdeling mag (in principe) niet worden uitbesteed.



Figuur 4: Raamwerk afweging in-huis/uitbesteden

De afweging of bepaalde activiteiten zelf moeten worden uitgevoerd (in-huis) dan wel beter kunnen worden uitbesteed, is in figuur 4 als volgt weergegeven:[16]

Risicoanalyse
Het is van belang dat een financiële onderneming die op structurele basis werkzaamheden uitbesteedt, de risico's die daarmee samenhangen analyseert. Risicoanalyse is een essentieel element om te beoordelen of de werkzaamheden wel of niet kunnen worden uitbesteed. Gedacht kan worden aan bijvoorbeeld procedures die worden gevolgd en maatregelen die kunnen worden genomen in geval van tekortschietende dienstverlening door de derde en calamiteiten. Het uitbesteden van werkzaamheden valt onder het operationeel risico aldus de Nota van toelichting op de open norm van artikel 29 Bpr.
Dit artikel luidt:
'…een clearinginstelling, kredietinstelling, verzekeraar, …, voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot het op structurele basis uitbesteden van werkzaamheden.'

Ik kan me voorstellen dat niet elke lezer bij dit artikel direct de associatie heeft met het uitvoeren van een risicoanalyse naar de uit te besteden werkzaamheden door de financiële onderneming èn het op grond daarvan inrichten van maatregelen/procedures om de risico's te mitigeren. Degenen die in het verleden audits hebben uitgevoerd op basis van de ROB of de RUV leggen dat verband waarschijnlijk wel. In de transponeringstabel Bpr – oude toezichtwetgeving (zie tabel 1 aan het einde van deze publicatie) zijn namelijk de artikelen met betrekking tot de risicoanalyse uit de ROB en de RUV gekoppeld aan artikel 29 Bpr. De gekoppelde artikelen uit de ROB zijn bijvoorbeeld:

- 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 (art 58 ROB).
- De instelling draagt zorg 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 (art. 60 ROB).
- De instelling werkt de beleidsuitgangspunten ter beheersing van uitbestedingrisico's nader uit in organisatorische en administratieve procedures en maatregelen en integreert deze in de systemen en de dagelijkse werkzaamheden van alle relevante geledingen (art 61 ROB)[iii].

Door gebruik te maken van de Nota van toelichting en de transponeringstabel kunnen de open normen uit de Wft enigszins worden geconcretiseerd.

Selectiefase
Voor de selectiefase zijn geen normen in de Wft opgenomen waaraan de IT-auditor moet toetsen. Het projectteam kan in

deze fase wel de hulp van de IT-auditor inroepen. Bijvoorbeeld in het kader van een due diligence onderzoek naar het in opzet vaststellen dat de dienstverlener aan de opgenomen regelgeving kan voldoen. In de praktijk is het niet altijd mogelijk (of erg kostbaar) om de interne regels aan de dienstverlener op te leggen. Vaak hebben deze partijen al eigen interne regelingen (gedragscodes en dergelijke) die hetzelfde doel dienen. Het is dan van belang vast te (laten) stellen of, en zo ja, waar afwijkingen bestaan tussen de interne regelingen van de financiële onderneming en die van de dienstverlener.[17]

Contractfase

De normen uit de Wft hebben in deze fase betrekking op de inhoud van de schriftelijke overeenkomst met de dienstverlener. Voor de *lessons learned* met betrekking tot uitbestedingovereenkomsten wordt verwezen naar de uitgave IT-REcht van 2006 waarin de door de Werkgroep juridisch Platform Outsourcing Nederland geïnventariseerde problemen integraal zijn weergegeven.[18]

In artikel 31 Bpr is een uitgebreide lijst verplichte onderwerpen voor de SLA opgenomen. Dit is niet geheel in lijn met het uitgangspunt van '*principle based*'. In de overeenkomst moet op grond van de Wft in ieder geval het volgende worden geregeld:

- de onderlinge informatie-uitwisseling, met inbegrip van afspraken over het beschikbaar stellen van informatie waarom de toezichthouders ter uitvoering van hun wettelijke taak verzoeken.
- de mogelijkheid voor de financiële onderneming om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt;
- de verplichting voor de derde om de financiële onderneming in staat te stellen blijvend te voldoen aan het bij of krachtens de wet bepaalde.
- de mogelijkheid voor de toezichthouders om onderzoek ter plaatse te doen of te laten doen bij de derde.
- de wijze waarop de overeenkomst wordt beëindigd, en de wijze waarop wordt gewaarborgd dat de financiële onderneming de werkzaamheden na beëindiging van de overeenkomst weer zelf kan uitvoeren of door een andere derde kan laten uitvoeren.

Wanneer de werkzaamheden worden uitbesteed aan een onderneming met een zetel in een lidstaat, die deel uitmaakt van de groep waartoe de financiële onderneming behoort, is een verlicht regime van toepassing. Dit betekent in ieder geval dat bovengenoemde vereisten niet in de SLA hoeven te worden opgenomen.

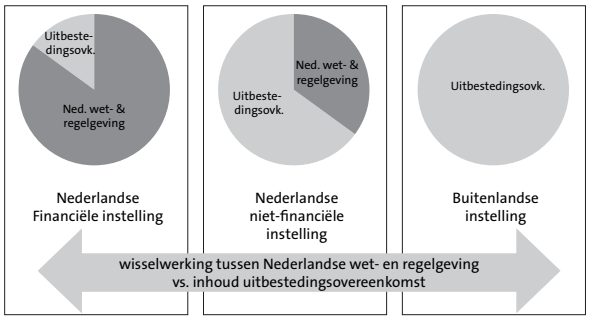
Financiële ondernemingen die al activiteiten hebben uitbesteed, doen er goed aan hun contracten te toetsen of deze wel volledig aan de vernieuwde regeling voldoen. Op grond van de overgangsregeling kunnen de bestaande uitbestedingovereenkomsten in stand blijven maar dienen ze na contractherziening wel te voldoen aan de in het besluit opgenomen vereisten.

Naar aanleiding van de in de analysefase uitgevoerde risicoanalyse is duidelijk geworden welke risico's de financiële onderneming loopt bij het uitbesteden van de werkzaamheden en welke maatregelen zij verwacht van de serviceorganisatie. Door deze verwachte maatregelen als vereisten in de SLA op te nemen worden de met uitbesteding verbonden risico's gemitigeerd. Een aantal van deze vereisten is op grond van artikel 31 Bpr al verplicht gesteld (zie hierboven).
De SLA is ook een instrument om vraag en aanbod tussen de klant en de leverancier bij het uitbesteden van diensten te synchroniseren, door daarin goede afspraken te maken over het gewenste niveau van dienstverlening. Een SLA biedt naast een bijdrage aan de doelen die met de uitbesteding worden nagestreefd (kostenreductie en/of kostenbeheersing, vergroting flexibiliteit, oplossen van een kennisprobleem, verdere focus op kerntaken, et cetera), een basis voor de beheersing van de dienstverlening. Enerzijds ontstaan door het bepalen en vastleggen van het gewenste niveau van dienstverlening (Quality of Service) en het meten van de gerealiseerde doelstelling mogelijkheden om op basis van objectieve cijfers sturing te geven aan die dienstverlening. Anderzijds wordt door overleg tussen de afnemer en de leverancier wederzijds inzicht in en begrip van eisen, wensen en mogelijkheid van de betrokken partijen verkregen. Dit ondersteunt het management in zijn steven naar een verbetering van effectiviteit en efficiency.[19]

De aandacht die in een uitbestedingovereenkomst moet worden besteed aan de relevante compliancerisico's is volgens Schouten ook afhankelijk van de serviceorganisatie. Zij onderscheidt drie uitbestedingsmogelijkheden, namelijk uitbesteding aan een:[20]

- Nederlandse financiële instelling;
- Nederlandse niet financiële instellingen; en
- buitenlandse instelling.

Volgens Schouten is er ten aanzien van de beheersing van de compliancerisico's een wisselwerking tussen de Nederlandse wet- en regelgeving enerzijds en de inhoud van de uitbestedingovereenkomst anderzijds. In figuur 5 is schematisch weergegeven dat naarmate de invloed van de Nederlandse wet- en regelgeving voor wat betreft het prudentieel- en/of gedragstoe-



Figuur 5: Wisselwerking Nederlandse wet- en regelgeving vs. Inhoud uitbestedingovereenkomst.

zicht afneemt, in de uitbestedingovereenkomst meer aandacht aan de relevante compliancerisico's moet worden besteed.

Transitiefase
Voor de transitiefase zijn geen normen in de Wft opgenomen waaraan de EDP-auditor kan toetsen.

Contractmanagement
Wat voorheen alleen voor de uitbestedende verzekeraar gold (art. 7 RUV) geldt nu ook voor de uitbestedende bank. Zij dient naast procedures en maatregelen ook te beschikken over *deskundigheid* om de uitvoering van de op structurele basis uitbestede werkzaamheden te kunnen beoordelen (art. 30 Bpr). In de ROB werd dit niet expliciet gevraagd.
Voor een adequate beoordeling van de uitbestede werkzaamheden dient de financiële onderneming te beschikken over voldoende informatie van de serviceorganisatie en dient de uitbestedende financiële onderneming over de deskundigheid te beschikken om die informatie te kunnen beoordelen.

Conclusie
Audits naar de rechtmatigheid van de uitbesteding van werkzaamheden door een financiële onderneming zijn compliance audits waarbij de open normen van onder andere de Wft door de IT-auditor moeten worden geïnterpreteerd. Dit betekent dat de auditor juridisch moet zijn onderlegd of in zijn auditteam over juridische kennis moet kunnen beschikken. Voor de Wft zijn de open normen nog niet uitgekristalliseerd. Voor de interpretatie van de open normen van de Wft en de onderliggende besluiten en regelingen kunnen naast de nota van toelichting op de besluiten voorlopig de oude toezichthouderregels zoals de ROB, de RUV en NRge2002 als basis dienen. ■

Tabel 1: Transponeringstabel Bpr - oude toezichtwetgeving (gebaseerd op: Toelichting op Bpr)[21]

Besluit prudentiële regels Wft (Bpr)	*Regeling Organisatie en beheer (ROB) van DNB*	*Regeling uitbesteding verzekeraars (RUV)*
HOOFDSTUK 5. UITBESTEDEN VAN WERKZAAMHEDEN **Bepalingen ter uitvoering van artikel 3:18, tweede en derde lid, van de wet**		
Artikel 27 1. Een financiële onderneming of bijkantoor als bedoeld in artikel 3:18, eerste lid, 3:22, 3:23, 3:25, 3:26 of 3:27, van de wet gaat niet over tot het uitbesteden van werkzaamheden indien die uitbesteding een belemmering kan vormen voor een adequaat toezicht op de naleving van het bij of krachtens het Deel Prudentieel toezicht financiële ondernemingen van de wet bepaalde. 2. Een clearinginstelling, kredietinstelling, verzekeraar of bijkantoor als bedoeld in artikel 3:18, tweede lid, 3:23, 3:26 of 3:27 van de wet 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 3 Beperkingen aan uitbesteding** Onverminderd artikel 2 zijn die vormen van uitbesteding, die de verantwoordelijkheid van de verzekeraar voor de organisatie en beheersing van bedrijfsprocessen en het toezicht daarop kunnen ondermijnen, niet toegestaan.
Artikel 28 Een clearinginstelling, kredietinstelling, verzekeraar of bijkantoor als bedoeld in artikel 27, tweede lid, gaat niet over tot het uitbesteden van werkzaamheden indien dat afbreuk doet aan de kwaliteit van haar onafhankelijke interne toetsing als bedoeld in artikel 17, vierde lid.	**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.	**Artikel 3 Beperkingen aan uitbesteding** Onverminderd artikel 2 zijn die vormen van uitbesteding, die de verantwoordelijkheid van de verzekeraar voor de organisatie en beheersing van bedrijfsprocessen en het toezicht daarop kunnen ondermijnen, niet toegestaan.
-	**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.	-

Besluit prudentiële regels Wft (Bpr)	*Regeling Organisatie en beheer (ROB) van DNB*	*Regeling uitbesteding verzekeraars (RUV)*
Artikel 29 Een clearinginstelling, kredietinstelling, verzekeraar of bijkantoor als bedoeld in artikel 27, tweede lid, voert een adequaat beleid en beschikt over procedures en maatregelen met betrekking tot het op structurele basis uitbesteden van werkzaamheden.	**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.	**Artikel 2 Beleid ter zake van uitbesteding** 1. De verzekeraar stelt beleid vast met betrekking tot de beheersing van risico's die samenhangen met de uitbesteding van bedrijfsprocessen. 2. Het beleid betreft in ieder geval: a. het bepalen dat de verzekeraar voldoende waarborgen verkrijgt voor het handhaven van een beheerste en integere bedrijfsvoering alsmede dat de uitvoerende organisatie maatregelen treft inzake fraudepreventie; b. het vaststellen dat de verzekeraar niet tot uitbesteding zal overgaan van bedrijfsprocessen indien niet aan onderdeel a wordt voldaan
	Artikel 60 De instelling draagt zorg 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.	**Artikel 4 Risicoanalyse** De verzekeraar draagt zorg voor een systematische analyse van risico's die samenhangen met de uitbesteding van bedrijfsprocessen. De analyse wordt uitgevoerd zowel op het niveau van de organisatie van de verzekeraar in zijn geheel als op het niveau van de onderscheiden bedrijfsonderdelen.
	Artikel 61 De instelling werkt de beleidsuitgangspunten ter beheersing van uitbestedingrisico's nader uit in organisatorische en administratieve procedures en maatregelen en integreert deze in de systemen en de dagelijkse werkzaamheden van alle relevante geledingen.	**Artikel 5 Procedures en maatregelen** 1. De verzekeraar draagt zorg voor de uitwerking en implementatie van het beleid in organisatorische en administratieve procedures en maatregelen. 2. De in het eerste lid bedoelde procedures en maatregelen omvatten in ieder geval: a. de procedures inzake de besluitvorming ten aanzien van een voorgenomen nieuwe of gewijzigde uitbesteding, waaronder de in artikel 4 bedoelde risicoanalyse; b. de beoordeling van de uitvoerende organisatie.
Artikel 30 Een clearinginstelling, kredietinstelling, verzekeraar of bijkantoor als bedoeld in artikel 27, tweede lid, beschikt over toereikende procedures, maatregelen, deskundigheid en informatie om de uitvoering van de op structurele basis uitbestede werkzaamheden te kunnen beoordelen.	**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.	**Artikel 6 Controle** De verzekeraar toetst regelmatig of de wijze waarop de uitbestede bedrijfsprocessen worden uitgevoerd nog in overeenstemming is met de gemaakte afspraken. Daartoe beschikt de verzekeraar over toereikende procedures, deskundigheid en informatie om de werkzaamheden van de uitvoerende organisatie op adequate wijze te kunnen beoordelen en zonodig bij te sturen.
Artikel 31 1. Een clearinginstelling, kredietinstelling, verzekeraar of bijkantoor als bedoeld in artikel 27, tweede lid, legt de overeenkomst met de derde waaraan de werkzaamheden op structurele basis worden uitbesteed schriftelijk vast. 2. In de overeenkomst wordt in ieder geval het volgende geregeld: a. de onderlinge informatie-uitwisseling, met inbegrip van afspraken over het beschikbaar stellen van informatie waarom de toezichthouders ter uitvoering van hun wettelijke taak verzoeken; b. de mogelijkheid voor de financiële onderneming of het bijkantoor om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt; c. de verplichting voor de derde om de financiële onderneming of het bijkantoor in staat te stellen blijvend te voldoen aan het bij of krachtens de wet bepaalde; en d. de mogelijkheid voor de toezichthouders om onderzoek ter plaatse te doen of te laten doen bij de derde; en e. de wijze waarop de overeenkomst wordt beëindigd, en de wijze waarop wordt gewaarborgd dat de financiële onderneming of het bijkantoor de werkzaamheden na beëindiging van de overeenkomst weer zelf kan uitvoeren of door een andere derde kan laten uitvoeren. 3. De toezichthouders maken slechts gebruik van de mogelijkheid, bedoeld in het tweede lid, onderdeel d, indien niet op andere wijze kan worden vastgesteld dat ten aanzien van de uitbestede werkzaamheden wordt voldaan aan het bij of krachtens de wet bepaalde.	**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/leverancier 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.	**Artikel 6 Controle** De verzekeraar toetst regelmatig of de wijze waarop de uitbestede bedrijfsprocessen worden uitgevoerd nog in overeenstemming is met de gemaakte afspraken. Daartoe beschikt de verzekeraar over toereikende procedures, deskundigheid en informatie om de werkzaamheden van de uitvoerende organisatie op adequate wijze te kunnen beoordelen en zonodig bij te sturen. **Artikel 7 Overeenkomst van uitbesteding** 1. De verzekeraar legt de afspraken met de uitvoerende organisatie inzake uitbesteding vast in een schriftelijke overeenkomst. Deze overeenkomst dient het geheel van relevante aspecten betreffende de uitbestede bedrijfsprocessen te omvatten, zoals aard, omvang, kwaliteit, tijdigheid, servicegraad, deskundigheid, informatievoorziening, eigendom van gegevens en verplichting tot naleving van relevante wet- en regelgeving. 2. In het geval van volmacht wordt in de in het eerste lid bedoelde overeenkomst vastgelegd dat de gevolmachtigd agent de financiële jaarrapportage over de volmacht voorziet van een verklaring van een accountant als bedoeld in artikel 2:393, eerste lid, van het Burgerlijk Wetboek. 3. De in het eerste lid bedoelde overeenkomst moet waarborgen dat de verzekeraar de uitbesteding van de bedrijfsprocessen onder bepaalde, van tevoren overeengekomen nauwkeurig omschreven omstandigheden kan beëindigen en dat de verzekeraar de desbetreffende bedrijfsprocessen zelfstandig kan voortzetten of elders kan onderbrengen. De beëindiging dient te zijn omgeven met financiële en uitvoeringstechnische waarborgen. 4. Als onderdeel van de in het eerste lid bedoelde overeenkomst verklaart en garandeert de uitvoerende organisatie, indien zij voor meer dan één opdrachtgever werkt, dat de gegevens en bestanden van de verschillende opdrachtgevers logisch te scheiden zijn, dat de privacyaspecten zijn gewaarborgd en dat de gescheiden informatieverstrekking naar de verschillende opdrachtgevers voldoende is gewaarborgd. 5. De in het eerste lid bedoelde overeenkomst moet waarborgen dat de uitvoerende organisatie aan de Pensioen- & Verzekeringskamer alle gevraagde inlichtingen - met inachtneming van eventueel bestaande wettelijke geheimhoudingsverplichtingen - verstrekt, de Pensioen- & Verzekeringskamer desgevraagd de toegang verschaft tot de relevante boeken en administratieve bescheiden en de aanwijzingen van de Pensioen- & Verzekeringskamer zal opvolgen die verband houden met de door de verzekeraar uitbestede bedrijfsprocessen.
Artikel 32 De artikelen 29 tot en met 31 zijn niet van toepassing op het uitbesteden van werkzaamheden aan ondernemingen met zetel in een lidstaat die deel uitmaken van de groep waartoe de financiële onderneming behoort.		

Noten

i De zeven oude toezichtwetten die in de Wft zijn opgenomen zijn: de Wet toezicht kredietwezen 1992 (Wtk 1992), de Wet toezicht verzekeringsbedrijf 1993 (Wtv 1993), de Wet toezicht natura-uitvaartverzekeringsbedrijf (Wtn), de Wet toezicht beleggingsinstellingen (Wtb), de Wet toezicht effectenverkeer 1995 (Wte 1995), de Wet financiële dienstverlening (Wfd) en de Wet melding zeggenschap en kapitaalbelang in effectenuitgevende instellingen (Wmz)

ii Regels inzake Chinese Walls hebben betrekking op de organisatie van een effecteninstelling en banken met effectenafdelingen. Deze organisaties moeten maatregelen treffen om belangenconflicten tussen de instellingen en hun cliënten of tussen cliënten onderling te voorkomen. Deze maatregelen moeten ook voorkomen dat binnen de organisatie koersgevoelige informatie wordt verspreid. Chinese Walls houden bijvoorbeeld in dat kredietverlening aan beursgenoteerde ondernemingen organisatorisch gescheiden moet zijn van de effectenbemiddeling en -advisering

iii Hoewel artikel 61 ROB niet in de transponeringstabel is opgenomen zou men kunnen stellen dat het ook onder 29 Bpr kan worden gelezen, aangezien het artikel een uitwerking is van artikel 58 ROB.

iv Hoewel artikel 61 ROB niet in de transponeringstabel is opgenomen zou je kunnen stellen dat, aangezien het artikel een uitwerking is van artikel 58 ROB, het ook onder 29 Bpr kan worden gelezen

Literatuurverwijzingen

1 Cazemier, F. 'Sourcing voor gevorderden', CIO Magazine, mei-juni 2007, nr. 3 2007, p. 100

2 Jongen, H.D.J., 'Inleiding Outsourcing' in Brunt, G. et al., (IT)Outsourcing, Elsevier 2004, p. 11

3 Jongen, H.D.J., 'Inleiding Outsourcing' in Brunt, G. et al., (IT)Outsourcing, Elsevier 2004, p. 12

4 Bloemer, A., 'Outsourcing in de financiële sector', Bank- en Effectenbedrijf, januari/februari 2004, p. 18

5 Rabobank, Handboek Outsourcing Rabofacet, juli 2004, versie 1.1, p. 9

6 Bakkers, R.W.A., 'De rol van de compliancefuncite in het uitbestedingsproces, Tijdschrift voor Compliance, 2006, nr 5, p. 141

7 Bolderhey, I.A.J en F. IJpeij, ´MiFID: zelfs bij 'business as usual' verandert er veel', EDP Auditor, jaargang 16, 2007 nr. 3

8 Ernst & Young Financial Services, 'Special Wet op het financieel toezicht', EYe on Finance, april 2007, p. 17

9 Openingstoespraak minister Zalm, Wft-seminar 2006, 17 januari 2006

10 AFM, Beleid en prioriteiten AFM, periode 2007 / 2009, p. 15

11 Wet van 28 september 2006, houdende regels met betrekking tot de financiële markten en het toezicht daarop (Wet op het financieel toezicht), Staatsblad, 2006, 475

12 De definitie van uitbesteden is gebaseerd op de inleidende toelichting bij paragraaf 2.6 van de Regeling organisatie en beheersing (Rob)3 en artikel 1 van de Regeling uitbesteding verzekeraars (Ruv)

13 TK 2005-2006, 28 709 , nr 34, Vijfde Nota van wijziging, p. 21

14 TK 28 709, Amendement

15 AFM, Beleid en prioriteiten AFM, periode 2007 / 2009, p. 19

16 Beleidskader uitbesteding Rabobank, versie 1.1, 2006, p. 3

17 Bakkers, R.W.A., 'De rol van de compliancefuncite in het uitbestedingsproces, Tijdschrift voor Compliance, 2006, nr 5, p. 141

18 Voulon, M.B., A.W. Duthler, 'IT-REcht – Automatiseringscontracten; een handreiking voor IT-auditors', Kluwer, december 2006, p. 31 – 32

19 Nederlandse vereniging van Banken (NVB) – Commissie EDP Auditing, Outsourcing; Handreiking Service Level Agreements (SLA) en Service Level Management, Amsterdam, 2e druk, maart 2005, p. 5

20 Schouten, L.E., ´Compliance: ook bij uitbesteding´, Tijdschrift voor Compliance, 2004, nr. 6, p. 136

21 Staatsblad 2006 519, p. 188