

De rol van de compliance-functie in het uitbesteding-proces

In een eerdere publicatie in dit tijdschrift – geschreven vanuit een toezichthouderperspectief – is het fenomeen uitbesteding van activiteiten en de relevante compliance-regels die daarmee samenhangen onder de aandacht gebracht.¹ Dit artikel behandelt uitbesteding vanuit het perspectief van de financiële instelling en beoogt antwoord te geven op de vraag hoe een financiële instelling kan borgen dat complianceaspecten adequaat zijn ingebed in uitbestedingprocessen. Of, om in risicomanagementstermen² te spreken: hoe kunnen de compliancerisico's rondom uitbesteding adequaat worden beheerst?

Alvorens deze kernvraag te beantwoorden schets ik allereerst kort het kader waarin dit artikel moet worden gelezen: wat is uitbesteding (§ 1)? Uit welke fasen bestaat het uitbestedingproces (§ 2)? Welke complianceregelings zijn relevant voor de financiële instelling³ in het kader van uitbesteding (§ 3)? Hoe past uitbesteding in het internationaal (toezicht)kader (§ 4)? Vervolgens beschrijf ik een overzicht van activiteiten die de compliancefunctie kan uitvoeren om complianceaspecten adequaat en gestructureerd in te bedden in uitbestedingtrajecten (§ 5). Ik beschrijf deze activiteiten van de compliancefunctie per fase van het uitbestedingproces. Het is van cruciaal belang dat de compliancefunctie tijdens uitbestedingprojecten nauw samenwerkt met de andere risicofuncties⁴; ook hierop ga ik in (§ 6). Verder sta ik stil bij een aantal actuele ontwikkelingen op het gebied van financiële regelgeving en in het bijzonder de bepalingen betreffende uitbesteding hierin (§ 7). Ik eindig dit artikel met enkele slotoverdenkingen en een samenvattende conclusie (§ 8).

1. Uitbesteding

In het kader van dit artikel hanteer ik de definitie uit de Regeling Organisatie en Beheersing (ROB) van De Nederlandsche Bank (DNB): '... het door andere groepsentiteiten of door onafhankelijke derden op structurele basis laten leveren van diensten, goederen of faciliteiten die deel uitmaken van de bancaire of daaraan ondersteuning verleende bedrijfsprocessen...'.⁵

In de ROB wordt nader toegelicht dat het niet uitmaakt of een uitbesteding plaatsvindt binnen of buiten de groep waartoe de financiële instelling behoort; beide vallen onder de term 'externe dienstverlener'. Verder blijkt dat incidentele inhuur van diensten buiten de definitie valt. Het onderscheid tussen bancaire en ondersteunende processen⁶ is als zodanig niet relevant; elke uitbesteding

dient zorgvuldig op zijn eigen merites te worden beoordeeld.

2. Fasen in het uitbestedingproces

In een uitbestedingproces kunnen de volgende fasen onderscheiden worden, waarbij ik tevens aangeef wat de belangrijkste activiteiten per fase zijn.⁷

- I. Voorbereiding (bepalen scope/haalbaarheid/vereisten, HR-plan en communicatieplan).
- II. Assessment (datacollectie, uitvoeren assessment, Target Operating Model(s), aanbevelingen).
- III. Selectie (Request for Information/Request for Proposal, interactie met dienstverleners, evaluatie van de respons, downselect).
- IV. Onderhandeling (commerciële onderhandeling, due diligence, finaliseren business case, concept-contract met overgebleven dienstverlener(s), ontwikkelen van adviesaanvraag aan de ondernemingsraad).
- V. Contracting (juridische onderhandeling, finaliseren contract, advies ondernemingsraad, voorbereiden van

* Richard Bakkers is werkzaam als manager bij Protiviti, een onderneming op het gebied van risk consulting. Dit artikel is op persoonlijke titel geschreven. Vragen of opmerkingen naar aanleiding van dit artikel kunt u zenden aan <richard.bakkers@protiviti.nl>.

1. Zie L.E. (Lisette) Schouten 'Compliance: ook bij uitbesteding' in *TvCo* 2004-6.
2. Waarmee ik de gedachte volg dat compliance een vorm is van risicomanagement, in het bijzonder het management van 'regulatory risks' of integriteitsrisico's.
3. Ik gebruik deze verzamelterm voor effecten(krediet)instellingen, banken en verzekeraars; ik behandel de relevante regelgeving dan ook met de focus op deze soorten financiële instellingen. De aanbevelingen in dit artikel zijn naar mijn mening echter evengoed bruikbaar voor bijvoorbeeld trustkantoren, tussenpersonen of pensioenfondsen.
4. Hiermee doel ik in het bijzonder op Internal Audit, (Operational) Risk Management, Juridische Zaken en (IT) Security.
5. Vergelijk de definitie in de Wet op het financieel toezicht (Wft): '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'. Ik verwijs naar paragraaf 7 voor een nadere verdieping over (eisen aan) uitbesteding in de Wft.
6. Strikt juridisch gezien is de ROB uitsluitend van toepassing op kredietinstellingen; voor de strekking van dit artikel kan hier echter ook 'verzekerings- en ondersteunende processen' of 'effecten- en ondersteunende processen' worden gelezen.
7. Niet toegespitst op de compliancefunctie; hiertoe verwijs ik naar paragraaf 5.

de transitie, inrichten 'Service Management Organisation').

- VI. Transitie (overdracht van personeel/informatie/hardware/software op 'as-is'-basis).
- VII. Transformatie (herinrichten van de uitbestede processen naar het model van de dienstverlener).
- VIII. Monitoring (monitoren van de prestaties van de dienstverlener, controleren of de overeengekomen service levels gehaald worden).

3. Relevante complianceregels betreffende uitbesteding

De Autoriteit Financiële Markten (AFM) baseert haar toezicht op bedrijfsvoering (waaronder ook uitbesteding valt) op de bepalingen uit artikel 24 van de Nadere Regeling gedragstoezicht effectenverkeer 2002 (NRg2002).⁸ Daarnaast is sinds januari 2004 de zogenaamde Interpretatieve mededeling uitbesteding (Imu) van AFM van kracht. Formeel zijn deze regelingen alleen van toepassing op effecten(krediet)instellingen. Kortgezegd volgt uit de NRg2002 en Imu⁹ dat uitbesteding moet worden gezien als een 'significante wijziging van de administratieve organisatie en het systeem van interne controle' waartoe het voornemen aan AFM moet worden gemeld. Door uitbesteding mag adequaat toezicht van AFM niet worden belemmerd. Verder moet de effecten(krediet)instelling nagaan of de dienstverlener in staat is de werkzaamheden volgens de geldende regelgeving uit te voeren. Voor verdere details over deze regels verwijs ik naar het eerder aangehaalde artikel van Lisette Schouten.

Ik refereerde al eerder aan de ROB, die formeel overigens uitsluitend van toepassing is op kredietinstellingen, van DNB. In essentie schrijft de ROB¹⁰ voor dat de kredietinstelling moet zorgdragen voor een 'systematische analyse van de risico's die samenhangen met de uitbesteding van werkzaamheden'. Voorts moet de kredietinstelling beleid formuleren ter beheersing van de risico's die samenhangen met het uitbesteden van werkzaamheden; dit beleid moet worden uitgewerkt in procedures en maatregelen. Een andere bepaling schrijft voor dat de afspraken moeten worden vastgelegd in een schriftelijke overeenkomst waarin in ieder geval moet zijn opgenomen dat DNB de bevoegdheid heeft om (ook rechtstreeks) informatie in te winnen bij de dienstverlener. Sinds de fusie van de Pensioen & Verzekeringkamer (PVK) met DNB is DNB ook de toezichthouder op de Regeling uitbesteding verzekeraars (Ruv). De Ruv lijkt zeer sterk op de ROB, maar gaat op een aantal punten meer in detail. Allereerst schrijft de Ruv expliciet voor dat de verzekeraar de mogelijkheid moet hebben om de uitbesteding te beëindigen op basis van 'nauwkeurig voorgedefinieerde condities'.¹¹ Ten tweede moet de dienstverlener data en files van haar verschillende klanten logisch scheiden en 'privacy en een geschieden informatievoorziening garanderen'.¹² Beide elementen moeten expliciet in de uitbestedingovereenkomst zijn opgenomen. Daarnaast bepaalt de Ruv expliciet dat de dienstverlener antifraudemaatregelen moet treffen.¹³

Voor dit artikel volstaat het om aan te nemen dat de bepalingen uit de Imu, ROB en Ruv dezelfde strekking

hebben en hetzelfde doel dienen, namelijk een 'beheerste' overgang van de werkzaamheden van de financiële instelling naar de dienstverlener.¹⁴ Enkele relevante detailverschillen tussen deze regelingen komen in paragraaf 5 aan de orde.

Naast deze externe regelgeving betreffende uitbesteding zijn ook interne regels/richtlijnen/beleidslijnen betreffende uitbesteding relevant in dit kader. Samen met de specifieke regelgeving die van toepassing is op de te outsourcen dienst, vormt al deze regelgeving de 'Compliance Chart' (overzicht van alle toepasselijke regelgeving) van het uitbestedingsproject in kwestie. Ik licht dit nader toe in paragraaf 5 onder sub I.

4. Uitbesteding in een internationaal (toezicht)kader

Omdat veel van de in de vorige paragraaf genoemde (Nederlandse) regelgeving is ontleend aan internationale 'standaarden', bespreek ik een aantal internationale publicaties op dit gebied. Veel van deze 'standaarden' vinden we terug in de Nederlandse regelgeving; vanuit die achtergrond lijkt enige aandacht nuttig.

Het in mijn optiek meest relevante werk in dit kader komt van het Basel Committee on Banking Supervision (BCBS; een van de comités van de Bank for International Settlements). Het BCBS heeft 'high-level principles' over uitbesteding gepubliceerd¹⁵, welke een antwoord geven op de vragen hoe financiële instellingen overtuigd kunnen zijn dat zij na uitbesteding hun bedrijfsrisico's blijven beheersen. Hoe weten zij dat ze (blijven) voldoen aan de toepasselijke regelgeving? Hoe kunnen zij dit aantonen wanneer de toezichthouder daarom vraagt? Sleutelwoorden in de principes – waarmee financiële instellingen de aan uitbesteding verbonden risico's kunnen mitigeren – zijn onder andere 'clear outsourcing policies', 'effective risk management programmes', 'contingency programs' en 'appropriate outsourcing contracts'.

De principes worden 'gedragen' door toezichthouders uit verscheidene EU-landen, evenals landen als Australië, de Verenigde Staten en Canada. Uiteraard levert nationale

8. Artikel 24 NRg2002 is een nadere uitwerking van artikel 17 jo. artikel 34 Besluit toezicht effectenverkeer 1995.

9. Feitelijk is de Imu een interpretatie van artikel 24, lid 3 NRg2002.

10. Ik ga in de paragrafen over de 'checklist' nader in op een aantal bepalingen uit de ROB. Voor een volledig overzicht van eisen ten aanzien van uitbesteding verwijs ik naar paragraaf 2.6 van de ROB.

11. Zie artikel 7.3 Ruv.

12. Zie artikel 7.4 Ruv.

13. Zie artikel 2.2a Ruv.

14. Of deze 'externe dienstverlener' al dan niet deel uitmaakt van dezelfde groep als de financiële instelling die uitbestedt, is in dit kader niet relevant; de bepalingen blijven hetzelfde (zie ook de definitie uit de ROB).

15. 'Outsourcing in Financial Services', Basel Committee on Banking Supervision, februari 2005 (omdat dit een 'Joint Forum'-publicatie is, gelden de principes ook voor verzekeraars en effecteninstellingen) (<<http://www.bis.org/publ/joint12.htm>>).

implementatie van de principes wel lokale verschillen op in zaken als specifieke verboden, toestemming, meldplichten, contracteisen etcetera. Het gaat echter te ver om in het kader van dit artikel in detail op deze verschillen in te gaan.¹⁶

Andere relevante internationale publicaties waarin uitbesteding wordt behandeld, noemen soortgelijke principes voor het mitigeren van aan uitbesteding verbonden risico's.¹⁷

5. De rol van de compliancefunctie in de verschillende fasen van het uitbestedingsproces – een checklist

Ik kom nu bij de kern van dit artikel, te weten de rol (en betrokkenheid) van de compliancefunctie in uitbestedingsprocessen. Het is van belang dat compliance aspecten op een gestructureerde wijze zijn ingebed in een uitbestedingsproces. Als hulpmiddel hiervoor presenteer ik een checklist¹⁸ die in de praktijk wordt gebruikt als leidraad voor de betrokkenheid van de compliancefunctie in uitbestedingsprojecten.

Het is van belang om de betrokkenheid van de compliancefunctie adequaat te documenteren en dit toe te (laten) voegen aan het totale projectdossier, dat ter beoordeling door relevante stakeholders¹⁹ beschikbaar moet zijn.

Eerst sta ik stil bij een aantal algemene aandachtspunten in dit kader die niet exclusief aan een specifieke fase van het uitbestedingsproces verbonden zijn.

Compliancebetrokkenheid (algemeen)

Om met een open deur te beginnen: het is van groot belang dat de compliancefunctie in een zo vroeg mogelijk stadium bij het uitbestedingsproject betrokken wordt. Dit om te voorkomen dat – naast het feit dat relevante compliance-regels betreffende uitbesteding mogelijk niet worden nageleefd – de compliancefunctie wellicht in een verregaande fase van het project op de rem moet trappen. Dit kan tot gevolg hebben dat de reputatie van Compliance als 'projectkiller' weer wordt gevoed, maar dit mag uiteraard nooit het naleven van regelgeving in de weg staan.

Hoe kritischer de scope van het uitbestedingsproject in kwestie²⁰, hoe meer aandacht moet worden geschonken aan risicoreductie, veiligheidsmaatregelen etcetera. Deze maatregelen kunnen kostbaar zijn en hebben daarmee een directe impact op de business case. Ook daarom is het van belang deze in een zo vroeg mogelijk stadium te definiëren.²¹

De betrokkenheid van Compliance kan bijvoorbeeld worden geborgd door opname van de rol van de compliancefunctie in het interne uitbestedingsbeleid en/of het outsourcing rulebook dat (project) management als leidraad gebruikt voor het inrichten van het uitbestedingsproject. Een ander adequaat middel is dat de compliancefunctie in een vroeg stadium door middel van een presentatie aan (project)management de complianceaspecten (toepasselijke regelgeving, rol toezichthouders, etcetera) rondom het desbetreffende uitbestedingsproject toelicht en daarmee de

toegevoegde (advies)waarde van Compliance op de kaart zet.

Een vroege betrokkenheid is ook een stuk 'zelfbescherming' voor de compliance officer. Immers, hij/zij is eerder en beter op de hoogte van de specifieke facetten van het project in kwestie, kan hierdoor tijdig proactief, sturend optreden en kan voorkomen dat hij/zij in de eindfase van een project (wellicht onvoorbereid) stapels papier ter beoordeling en/of ter accordering krijgt voorgelegd.

Contacten met/informeren van toezichthouders

Hoewel niet iedere intentie tot uitbesteding direct aan de toezichthouder(s) hoeft te worden gemeld²², komt er hoe dan ook een moment dat zij geïnformeerd moet(en) worden.²³ Hoe kritischer de scope van het project in kwestie, hoe vroegtijdiger de toezichthouder(s) geïnformeerd moet(en) worden. Net als bij de noodzakelijke vroegtijdige betrokkenheid van de compliancefunctie zoals hiervoor beschreven, voorkomt een tijdige betrokkenheid van de toezichthouder(s) dat in een latere fase van het project op de rem moet worden getrapt.

Indien zowel AFM als DNB betrokken zijn²⁴, adviseer ik om AFM en DNB te verzoeken hun betrokkenheid/beoordeling onderling te coördineren. In de praktijk blijkt dat AFM en DNB per project afspreken welke toezichthouder het voortouw neemt en hoe zij onderling over de voortgang communiceren.

AFM beoordeelt in de verschillende fasen van het project sleuteldocumentatie zoals de business case, projectorganisatie en -planning en rapportages.²⁵ DNB beoordeelt met een soortgelijke bril, met (eveneens) een bijzondere aan-

16. Voor een eerste inzicht in nationale benaderingen van uitbesteding door toezichthouders verwijs ik naar de tabel op pagina 9–11 in het eerdergenoemde rapport 'Outsourcing in Financial Services'.

17. 'The High Level Principles on Outsourcing', The Committee of European Banking Supervisors, april 2004 (consultatie document) (<http://www.c-eps.org/Consultation_papers/CP02.htm>); 'Compliance and the compliance function in banks', april 2005, p. 15–16 (<<http://www.bis.org/publ/bcbs113.htm>>).

18. In paragraaf 8 is deze in tabelvorm weergegeven.

19. Internal Audit, externe accountant, toezichthouders, etc.

20. Voor een model/hulpmiddel om dit te bepalen verwijs ik naar <http://www.nl.capgemini.com/resources/thought_leadership/the_outsourcing_report> (pagina 9 en 10).

21. Dit geldt niet alleen voor compliance, maar ook voor risk management.

22. Veel uitbestedingsprojecten komen immers niet verder dan een inventarisatie van de haalbaarheid.

23. Hierbij moet worden aangetekend dat de ROB formeel geen meldplicht bevat. DNB verwacht echter dat de financiële instelling DNB over 'nieuwe, van materieel belang zijnde, vormen van uitbesteding zo spoedig mogelijk na de besluitvorming zal informeren'.

24. Dit kan gelden voor effectenkredietinstellingen, maar met de inwerkingtreding van het 'effectentypisch gedragstoezicht' kan dit ook voor andere financiële instellingen gelden.

25. Zie L.E. Schouten 'Compliance: ook bij uitbesteding' in *TvCo* 2004-6, p. 138 voor een uitgebreide opsomming.

dacht voor de project governance en de rol en adequate betrokkenheid van de verschillende risicofuncties.

Van belang is om te melden dat er wel een belangrijk verschil is tussen AFM en DNB, in de zin dat AFM haar expliciete schriftelijke goedkeuring moet verlenen voor de transitie naar de dienstverlener²⁶ in het geval dat AFM het voortouw neemt in het beoordelingsproces. Dit zal in de regel het geval zijn bij uitbesteding van effecten(gerelateerde)diensten door effecten(krediet)instellingen. In de praktijk komt het erop neer dat AFM vóór ondertekening van de overeenkomst haar schriftelijke goedkeuring moet hebben gegeven. In de praktijk blijkt dat indien AFM tijdig wordt geïnformeerd en tussentijds van adequate informatie wordt voorzien, zij minder tijd neemt dan de termijn van zes weken die AFM formeel heeft voor het beoordelen van een dergelijke goedkeuring.²⁷ In dergelijke situaties kan AFM binnen één tot twee weken na finale overeenstemming met de dienstverlener haar formele goedkeuring aan de financiële instelling verstrekken.

I. Voorbereidingsfase

In deze fase is het voor de compliancefunctie allereerst van belang om de bovengenoemde algemene betrokkenheid te borgen. Daarnaast is het van belang dat de compliance scope wordt bepaald, wat zijn gestalte krijgt in de vorm van een Compliance Chart.

Compliance Chart behorende bij het uitbestedingsproject

Zoals eerder genoemd is een Compliance Chart een overzicht van alle toepasselijke²⁸ regelgeving. Per uitbestedingsproject dient een overzicht van de volgende typen regelgeving te worden opgesteld:

- Externe regelgeving betreffende uitbesteding (afhankelijk van de aard van de financiële instelling en de aard van de dienst: Imu en/of ROB en/of Ruv²⁹).
- Interne regels/richtlijnen/beleidslijnen (interne regelingen) betreffende uitbesteding.
- Specifieke regelgeving die van toepassing is op de uit te besteden dienst.³⁰

De compliancefunctie heeft een leidende rol in het opstellen van de Compliance Chart en in het borgen dat de financiële instelling en de dienstverlener aan de opgenomen regelgeving (gaan) voldoen. Dit 'borgen' is overigens gemakkelijker gezegd dan gedaan.³¹ In de eerste plaats moet de compliancefunctie vaststellen in hoeverre het bedrijfsonderdeel zelf compliant is met deze regelgeving.³² Daarnaast moet de compliancefunctie gaan bepalen hoe zij in opzet gaat vaststellen dat de dienstverlener aan de opgenomen regelgeving kan voldoen. In de praktijk is het niet altijd mogelijk (of erg kostbaar) om interne regels aan de dienstverlener op te leggen. Vaak hebben deze partijen al eigen interne regelingen (gedragscodes en dergelijke) die hetzelfde doel hebben. Het is dan van belang om vast te (laten) stellen of en waar afwijkingen bestaan tussen de interne regelingen van de financiële instelling en die van de dienstverlener. De compliancefunctie speelt een belangrijke rol bij het bepalen en adviseren of de afwijkingen acceptabel zijn, waarbij externe regelgeving ten aanzien van het desbetreffende onderwerp van regelgeving uiter-

aard als het minimumniveau moet worden aangehouden. Met andere woorden, de interne regelgeving van de dienstverlener mag best afwijken van die van de financiële instelling in kwestie, maar mag nooit onder het niveau van de toepasselijke externe regelgeving liggen.

Zonder volledig te willen zijn, blijkt uit ervaring dat (naast de in- en externe regelgeving betreffende uitbesteding) de volgende onderwerpen in ieder geval deel moeten uitmaken van een Compliance Chart bij een uitbestedingsproject van een financiële instelling:

- gedragscode(s);
- screenen van personeel;
- incidentmanagement en -rapportering;
- verwerken van persoonsgegevens/privacy;
- insiders/privébeleggingstransacties (in geval van een effecten(krediet)instelling);
- witwassen van geld/terrorismefinanciering.

De compliance issues waarmee de financiële instelling te maken krijgt, de mate van bekendheid van de dienstverlener met de regelgeving die van toepassing is op financiële instellingen en daarmee de inspanningen die de financiële instelling moet verrichten om te borgen dat de dienstverlener aan de opgenomen regelgeving kan voldoen, hangen mede af van de keuze van de dienstverlener.³³ Dit geldt ook voor de mate van detail om dit in de uitbeste-

26. Formeel: voor de 'significante wijziging in de administratieve organisatie en het systeem van interne controle'.

27. Dit volgt uit artikel 17 jo. artikel 34 Besluit toezicht effectenverkeer 1995.

28. In dit kader doel ik op alle op de financiële instelling van toepassing zijnde regelgeving, die in scope van de compliancefunctie is; immers, in veel gevallen is (lang) niet alle regelgeving in scope van Compliance (zo is arbeidsrechtelijke en fiscaal- en accountinggerelateerde regelgeving in mijn ervaring expliciet buiten de scope van Compliance gesteld).

29. Zoals eerder vermeld, focus ik in dit artikel op effecten(krediet)instellingen, banken en verzekeraars. Voor regelgeving over uitbesteding door trustkantoren en tussenpersonen verwijs ik naar de toelichting op artikel 7, 8, 9, 10 en 11 bij de Regeling integrale bedrijfsvoering Wet toezicht trustkantoren resp. artikel 39 Wet financiële dienstverlening. Voor zover ik weet zijn er geen expliciete regelgeving van toepassing op uitbesteding door pensioenfondsen.

30. Dit is typisch dienstafhankelijk. Ter illustratie: bij het uitbesteden van de effectenadministratie moeten de relevante artikelen uit de NRG2002 over de effectenadministratie worden meegenomen; bij het uitbesteden van (delen van) cliëntacceptatie moet regelgeving over customer due diligence en privacy worden meegenomen.

31. Zie in dit kader ook L.E. Schouten 'Compliance: ook bij uitbesteding' in *TvCo* 2004-6, p. 136:

'De (directie van de) uitbestedende instelling blijft verantwoordelijk en aansprakelijk voor de uitbestede taken. De uitbestedende instelling moet zich aantoonbaar inspannen om aan de eisen van de NRG2002 [RB: en andere relevante regelgeving] te blijven voldoen'.

32. Deze vraag zal de dienstverlener ook stellen in het due diligence/onderhandelingsproces.

33. Ik doel in dit kader op de keuze tussen een dienstverlener die al dan niet zelf ook een financiële instelling is en in Nederland, in een EU-land of in een ander land gevestigd is. Ik verwijs verder naar L.E. Schouten 'Compliance: ook bij uitbesteding' in *TvCo* 2004-6, p. 135-136, voor uitgebreide informatie hierover.

dingovereenkomst te regelen. Immers, indien wordt uitbesteed aan een andere Nederlandse financiële instelling rust op deze instelling (nagenoeg³⁴) dezelfde regelgeving. Hieraan hoeft dan in de assessment- en onderhandelings-/contractfase minder aandacht te worden besteed. Aan de andere kant van het spectrum bevindt zich de niet-financiële dienstverlener die is gevestigd in een niet-EU-land, waarbij relatief veel aandacht moet worden besteed om de relevante compliancerisico's af te dekken.

II. Assessmentfase

Onderdeel van het totale assessment is in ieder geval het uitvoeren van een risicoanalyse.

Risicoanalyse

De ROB verplicht de financiële instelling om een analyse van risico's die samenhangen met de uitbesteding van werkzaamheden uit te voeren.³⁵

Afhankelijk van de situatie (zoals de aard van de instelling, aard van het project) kiest men voor een specifieke compliancegerelateerde risicoanalyse of voor een risicoanalyse waarin compliance als één van de onderwerpen wordt meegenomen. Het verdient de sterke aanbeveling om gebruik te maken van tools die al door (Operational) Risk Management worden gebruikt³⁶ en om de expertise van (Operational) Risk Management te gebruiken tijdens het uitvoeren van de risicoanalyse.

Naast deelnemer aan risicoworkshops kan de compliancefunctie ook optreden als zogenaamde 'devil's advocate' tijdens dergelijke workshops. Dit is een rol die de workshop(leider) ondersteunt door het confronteren en uitdagen van de deelnemers, bijvoorbeeld met betrekking tot inconsistenties of onvolledigheid van input en door het stellen van 'waarom'-, 'wanneer-', 'wat-', 'wie-', 'hoe'-vragen. Dit met het doel om van de deelnemers meer risico te horen of om de genoemde risico's adequater te kunnen beoordelen.

Ook heeft de compliancefunctie een rol om compliance-specifieke kennis over te dragen/toe te lichten tijdens de workshops.

Het resultaat van de risicoworkshop(s) is een overzicht van geïdentificeerde risico's, een inschatting van de waarschijnlijkheid en impact per risico (risicoclassificatie) evenals definiëren van risicomitigerende maatregelen per risico. Ook hier is een rol voor de compliancefunctie neergelegd in die zin dat deze een rol speelt bij het implementeren van de risicomitigerende maatregelen (en in sommige gevallen ook zelfstandig 'person-to-act' is) en bij het bewaken van de opvolging ervan.

III. Selectiefase

In deze fase worden dienstverleners geselecteerd voor nadere analyse. In eerste instantie wordt via een zogenaamd 'Request for Information' (RFI) aan een aantal dienstverleners en later via een zogenaamd 'Request for Proposal' (RFP) aan een overgebleven, kleiner aantal dienstverleners een beeld verkregen of en in hoeverre de dienstverleners de diensten tegen de vastgestelde criteria

kunnen leveren. De compliancefunctie moet in deze fase betrokken zijn bij de beoordeling van de respons van de dienstverleners op de compliancegerelateerde onderwerpen.

In de praktijk wordt deze beoordeling vaak gekwantificeerd door middel van scores. Op basis van de (gewogen) 'scores' van Compliance en de andere zogenaamde betrokken functies (zoals HR, Finance, Technical, Risk Management, Juridische Zaken, etcetera) wordt dan bepaald welke dienstverleners overgaan naar de volgende fase. Uiteraard moet de complianscore voldoende zwaar meewegen in dit scoringsproces.

IV. Onderhandelingsfase

Met de overgebleven dienstverleners worden commerciële onderhandelingen gestart. In deze fase kan het vóórkomen dat de compliancefunctie wordt gevraagd een mening/advies te geven over aan compliancegerelateerde vragen/opmerkingen vanuit het onderhandelingssteam.

In de onderhandelingsfase wordt ook een start gemaakt met de adviesaanvraag aan de ondernemingsraad. Het komt regelmatig voor dat – gezien de nauwe betrokkenheid in het project – de compliancefunctie wordt verzocht formeel akkoord te geven ('sign-off') op het indienen van de adviesaanvraag. Een beoordeling van deze adviesaanvraag is dan ook vereist.

V. Contractfase

In deze fase ligt de nadruk op (commercieel-)juridische onderhandelingen. Net als in de vorige fase kan de compliancefunctie een adviesrol vervullen over compliancegerelateerde vragen/opmerkingen vanuit het onderhandelingssteam.

In deze fase wordt ook de uitbestedingovereenkomst gefinaliseerd.

De uitbestedingovereenkomst

Naast het feit dat externe regelgeving dit expliciet voorschrijft³⁷, is uitbesteding in de regel een dermate kritische en complexe stap, dat vastlegging van de afspraken in een schriftelijke overeenkomst noodzakelijk is.

34. Afhankelijk van de aard van die financiële instelling.

35. Zie artikel 60 van de ROB: 'De analyse wordt uitgevoerd zowel op instellingsbrede basis als op het niveau van de onderscheiden bedrijfsonderdelen. Risicoanalyse is een continu proces, waarbij ten aanzien van uitbesteding op systematische wijze rekening dient te worden gehouden met de risico's van bestaande uitbestedingen, evenals van wijzigingen daarin en van nieuwe vormen van uitbesteding. Vooral daar waar uitbesteding plaatsvindt van werkzaamheden op IT-terrein (zie ook paragraaf 2.5 ROB) dienen de risico's van de snelle veranderingen op dat terrein in de risicoanalyse te worden betrokken.'

36. Denk hierbij aan de Business Impact Analysis en de Risk (and Compliance) & Control Self Assessment (workshop).

37. Zie onder meer artikel 62 van de ROB.

De compliancefunctie speelt ook in deze fase een belangrijke adviserende rol, omdat in de praktijk namelijk blijkt dat niet als vanzelfsprekend mag worden aangenomen dat zaken als compliance governance (aansturing/overleg) en compliance reporting in de (concept)overeenkomst zijn opgenomen. Dit terwijl het na transitie wel degelijk van groot belang is om formeel en periodiek met de dienstverlener te spreken over compliance(ontwikkelingen), rapportages te ontvangen over compliance gerelateerde issues, etcetera.

Naast deze rol moet de compliancefunctie ook vaststellen (dan wel zorgen dat deze in de checklist van juridische zaken zijn opgenomen) dat een aantal formele zaken adequaat in de uitbestedingovereenkomst zijn opgenomen:

- Het recht van toezichthouders om 'informatie in te winnen omtrent de uitbestede werkzaamheden bij de externe dienstverlener/leverancier'.³⁸
- De mogelijkheid om de uitbesteding te beëindigen op basis van nauwkeurig voorgedefinieerde condities, waaronder financiële en implementatietechnische (alleen de Ruv spreekt expliciet van deze verplichting, maar ik ga ervan uit dat dit in alle gevallen van toepassing is).
- De dienstverlener moet data en files van haar verschillende klanten logisch scheiden en privacy en een gescheiden informatievoorziening garanderen (ook hierbij geldt dat alleen de Ruv expliciet deze verplichting geeft, maar ik ga ervan uit dat ook dit in alle gevallen van toepassing moet zijn).

Ook moet de compliancefunctie vaststellen dat de regelgeving zoals opgenomen in de Compliance Chart is 'verwerkt' in de (bijlagen bij de) uitbestedingovereenkomst en dat daarin dwingend genoeg is bepaald dat de dienstverlener blijvend aan deze regelgeving (én dus ook aan de toekomstige veranderingen daarin!) moet voldoen.

In de contractfase wordt ook gestart met de voorbereiding van de transitie, waaronder het inrichten van de zogenaamde 'Service Management Organisation' (SMO). De SMO is het bedrijfsonderdeel dat 'achterblijft' bij de financiële instelling na transitie. De SMO heeft taken als contract- en servicemanagement onder zich, alsook het monitoren van de verrichte diensten en het dagelijks contact/de dagelijkse communicatie met de dienstverlener. Het is in deze fase van belang dat de compliancefunctie betrokken is bij de inrichting van de SMO om te borgen dat complianceaspecten voldoende aandacht krijgen binnen de SMO.

Indien AFM het voortouw neemt bij het beoordelen van het uitbestedingsproject, is dit ook de fase waarin zij haar formele, schriftelijke goedkeuring moet geven.

VI. Transitiefase

In deze fase worden de activiteiten in scope (al dan niet gefaseerd) aan de dienstverlener 'as-is' overgedragen. Voor alle betrokkenen (en dus ook voor Compliance) bij het project is het van belang om de overgang zorgvuldig

te monitoren en eventuele problemen naar de stuurgroep te escaleren.

VII. Transformatiefase

In deze fase wordt toegewerkt naar de eindsituatie waarbij de uitbestede processen worden getransformeerd naar de staande processen van de dienstverlener. Hier is een grote betrokkenheid van Compliance vereist aangezien hier weeffouten kunnen ontstaan. De nieuwe processen dienen aan alle eisen te voldoen waaraan de uitbestede processen 'as-is' moeten voldoen.

VIII. Monitoringfase

Na transitie blijft de financiële instelling verantwoordelijk en aansprakelijk voor de uitbestede dienst. De financiële instelling zal dan ook actief moeten (laten³⁹) monitoren dat de dienstverlener aan de contractvoorwaarden/service levels voldoet. De compliancefunctie speelt een adviserende, coördinerende rol bij het (laten) monitoren van de compliancegerelateerde issues in dit kader, het beoordelen van hieruit volgende rapportages en opvolgen van verbeteracties. De toezichthouders verwachten van de financiële instelling dat 'belangrijke problemen met betrekking tot de organisatie of de prestaties van de externe dienstverlener/leverancier' aan hen worden gemeld.⁴⁰

Naast monitoring is het in deze post-transitiefase van belang om ontwikkelingen op het gebied van compliance (regelgeving) te volgen en hierover structureel te communiceren met de dienstverlener. Een wijziging in regelgeving kan aanleiding geven tot de aanpassingen aan de uitbestedingovereenkomst. Compliance zal de SMO hierover moeten inlichten en adviseren.

6. Samenwerking met de andere risicofuncties

De (advies)rol van Compliance mag geen 'one-function'-show zijn, daarvoor is het proces te complex en raken de compliance issues in veel gevallen aan de andere risicodisciplines. Het is dan ook van cruciaal belang dat de compliancefunctie tijdige en adequate afstemming zoekt met de andere risicofuncties.

Hieronder volgt een overzicht van de belangrijkste afstemmings-/samenwerkingspunten per risicofunctie (tot aan transitie):

- Internal Audit: met name moet afstemming worden gezocht over de 'right-to-audit'-bepalingen in de overeenkomst, de zogenaamde 'Third Party Mededeling' en - indien van toepassing - de bepalingen/afspraken ten aanzien van de Sarbanes-Oxley Act. Het is ook raadzaam om de expert opinion van Internal Audit te vragen over de uitgevoerde risicoanalyse(s) en mitigerende maatregelen.

38. Citaat uit de toelichting op artikel 62 van de ROB.

39. Door de Compliance- (of soortgelijke) afdeling of interne accountantsdienst van de dienstverlener, door de externe accountant, etcetera.

40. Zie de toelichting bij artikel 64 van de ROB.

- (Operational) Risk Management: met deze functie is het van belang om samen te werken bij de uitvoering en opvolging van de risicoanalyse(s).
- Juridische Zaken: deze partij is leidend bij het opstellen van en onderhandelen over de totale uitbestedingovereenkomst. De compliancefunctie moet tijdig input geven over de compliancegerelateerde bepalingen in de overeenkomst.
- (IT) Security: indien in het kader van de uitbesteding (delen van) automatisering wordt geoutsourced is het van belang om aansluiting te zoeken bij (IT) Security. Hierbij is het relevant om op te merken dat in de externe regelgeving specifieke eisen worden gesteld aan (IT) Security⁴¹, eisen waaraan de dienstverlener ook zal moeten voldoen. De compliancefunctie adviseert welke van deze eisen van belang zijn voor het desbetreffende uitbestedingsproject.

Na transitie van de activiteiten moet de compliancefunctie met deze disciplines blijven samenwerken en blijven communiceren over monitoring(resultaten).

7. Ontwikkelingen op het terrein van financiële regelgeving⁴²

Op het moment van schrijven van dit artikel⁴³ speelt een aantal belangrijke ontwikkelingen op het gebied van regelgeving, waarin nadrukkelijk bepalingen over uitbesteding zijn opgenomen. De belangrijkste ontwikkelingen spelen in het kader van de invoering van de Wet op het financieel toezicht (Wft) en de implementatie van de Markets in Financial Instruments Directive ('MiFID'). De invoering van de Wft staat gepland voor 1 januari 2007; de MiFID zal naar verwachting in januari 2008 in de Nederlandse financiële wetgeving (op dat moment de Wft) geïmplementeerd zijn.⁴⁴ Bij het ontwerp van de Wft wordt gedeeltelijk al rekening gehouden met de implementatie van de MiFID.

Zowel voor afgeronde projecten als voor projecten die (gaan) lopen, is het van belang om nu al te anticiperen op deze geplande wijzigingen; dat geldt uiteraard niet alleen voor de bepalingen over uitbesteding.

Wft

Kortgezegd vervangt de Wft acht bestaande financiële wetten (en onderliggende regelgeving) om de omkanteling van sectoraal naar functioneel toezicht nu ook in de financiële wetgeving door te voeren.

In hoofdstuk 2 (Prudentieel toezicht financiële ondernemingen) en hoofdstuk 4 (Gedragstoezicht financiële ondernemingen) van de Wft zijn algemene bepalingen over uitbesteding opgenomen.⁴⁵ In de huidige opzet van de Wft worden twaalf algemene maatregelen van bestuur (AMvB's) onder de Wft 'gehangen'. In AMvB 5 (Besluit prudentiële regels financiële ondernemingen; Bpr) en 8 (Besluit gedragsregels financiële ondernemingen; Bgfo) zijn specifieke voorschriften over uitbesteding opgenomen.⁴⁶

Mijn eerste conclusie (op basis van de meest actuele⁴⁷ tekst van de wet) is dat er geen 'verzwaringen' in toezicht

op/eisen aan uitbesteding worden doorgevoerd bij invoering van de Wft. Sterker nog, door het vervallen van de Imu, ROB en Ruv⁴⁸ vervalt een groot aantal specifieke eisen aan uitbesteding die momenteel in deze toezichthouderregels zijn opgenomen; zo is er bijvoorbeeld geen specifieke eis meer tot het uitvoeren van een risicoanalyse. Wat wel overblijft, is de melding aan de toezichthouder.⁴⁹ Uit de Wft⁵⁰ en de AMvB's⁵¹ blijkt echter dat ten aanzien van uitbesteding géén regels worden gesteld ten aanzien van wanneer wijzigingen moeten worden gemeld, dat DNB (of AFM) toestemming moet verlenen, of dat DNB (of AFM) voorwaarden kan stellen. Dit is in ieder geval ten opzichte van de Imu een 'verlichting'. Ik ben overigens van mening dat in het kader van een goede relatie met en informatievoorziening aan de toezichthouder het van belang is om – zeker bij kritische uitbesteding – deze tijdig op de hoogte te stellen.

Tijdens het consultatieproces van de Wft is mede door lobby van brancheorganisaties bewerkstelligd dat de Wft alleen van toepassing is op 'wezenlijke' uitbesteding.⁵² Ook is bewerkstelligd (dit is nog niet in de tekst opgenomen, maar wel door het Ministerie van Financiën toegezegd) dat de eisen alleen zullen gelden voor externe (bedoeld in tegenstelling tot interne) uitbesteding. Ook dit zou een 'verlichting' ten opzicht van de huidige regelgeving zijn, aangezien de ROB externe en interne uitbesteding gelijkstelt qua eisen.⁵³

Een opvallend verschil tussen de algemene bepalingen in het prudentiële en het gedragsdeel van de wet (deel 2 resp. 4 Wft) is het feit dat het prudentiële deel van toepassing is op alle financiële ondernemingen waaraan de vergunning door de prudentieeltoezichthouder (DNB) wordt verleend.⁵⁴ In tegenstelling hiermee wordt in het gedragsdeel (behoudens de algemene bepaling van artikel 4:16 lid 1 Wft, die inhoudt dat de financiële onderneming

41. Zie bijvoorbeeld paragraaf 2.5 van de ROB en artikel 4.27 Bijlage 4 NRg2002.

42. Ik dank mr. R.K. Pijpers, jurist Regulatory Affairs bij ING Groep, voor zijn opmerkingen op eerdere versies van deze paragraaf.

43. September 2006.

44. Hoewel de Europese Unie een deadline van 1 november 2007 heeft opgelegd.

45. Zie artikel 2:46 resp. artikel 4:16 Wft.

46. Zie artikel 26–28 Bpr resp. artikel 36 Bgfo.

47. September 2006.

48. Met de invoering van de Wft 'vervallen' de huidige toezichthouderregels, waaronder ook de Imu, ROB en Ruv; het is nog niet duidelijk wat de impact van de Wft is op de huidige beleidslijnen van de toezichthouders.

49. Hoewel het door de vele kruisverwijzingen uitermate lastig is om de grondslag hiervoor te vinden (met dank aan mr. F. van Laar, jurist Regulatory Affairs bij ING Groep): artikel 2:57 lid 1 Wft jo. artikel 1a:11 lid 3 Wft jo. artikel 8.1 onderdeel k (AMvB 4); N.B. dit betreft de grondslag voor kredietinstellingen, voor de overige financiële instellingen zijn soortgelijke 'speuracties' noodzakelijk.

50. Artikel 2:57 lid 3 Wft resp. artikel 4:26 lid 3 Wft.

51. Hoofdstuk 6 Bpr resp. hoofdstuk 9 Bgfo.

52. Zie artikel 1.1 Wft (definities).

53. Zie paragraaf 1.

54. Kredietinstellingen, verzekeraars en clearinginstellingen.

moet zorgdragen dat de dienstverlener de van toepassing zijnde regelgeving naleeft) alleen ingegaan op beheerders en bewaarders van beleggingsinstellingen. Zoals blijkt uit de toelichting⁵⁵ wordt voor beleggingsondernemingen en financiële dienstverleners (waaronder effecteninstellingen) 'niet voorzien in een grondslag voor het stellen van [RB: nadere] regels met betrekking tot de beheersing van risico's die verband houden met de uitbesteding of een met de derde af te sluiten overeenkomst'. Als reden wordt vermeld dat de Wet toezicht effectenverkeer 1995 (Wte 1995) en de Wet financiële dienstverlening (en daarop gebaseerde regelgeving) niet voorzien in dergelijke regels. Mij lijkt deze redenering nogal 'wankel' aangezien de Wft mede tot doel heeft het toezicht op de verschillende financiële instellingen zo veel mogelijk te harmoniseren.

In de specifieke voorschriften van het Bpr is opgenomen dat de uitbesteding schriftelijk moet worden overeengekomen. De eisen aan een dergelijke uitbestedingsovereenkomst⁵⁶ wijken op punten af van de desbetreffende bepalingen in de ROB en Ruv. Het is dan ook noodzakelijk om bestaande uitbestedingsovereenkomsten en concept-overeenkomsten in het kader van lopende projecten hierop na te zien en eventueel aan te passen.^{57, 58}

In het Bgfo zijn zoals eerder gemeld ten aanzien van uitbesteding alleen specifieke voorschriften voor beheerders en bewaarders van beleggingsinstellingen opgenomen. Hierin is onder meer opgenomen dat het bepalen van het beleggingsbeleid van een beleggingsinstelling niet mag worden uitbesteed. Verder moet de uitbesteding schriftelijk worden overeengekomen.⁵⁹ Aan een dergelijke overeenkomst worden (in tegenstelling tot het Bpr) geen nadere eisen gesteld, hoewel in de overige leden van artikel 36 Bgfo wel degelijk een aantal aanknopingspunten is opgenomen voor zaken die naar mijn mening expliciet in de overeenkomst moeten worden opgenomen.

MiFID

De MiFID en de op de MiFID gebaseerde uitvoeringsmaatregelen vervangen de huidige Investment Services Directive (ISD). De ISD is de Europese richtlijn die ten grondslag ligt aan de Wte 1995. De MiFID zal evenals de ISD uitsluitend van toepassing zijn op effecten(krediet)instellingen.

AFM heeft in april 2006 een brochure⁶⁰ uitgebracht, waarin in mijn optiek helder is aangegeven welke eisen de MiFID zal stellen aan uitbesteding: 'Ten aanzien van uitbesteding van operationele taken⁶¹ vereist de MiFID dat de beleggingsonderneming redelijke maatregelen neemt om het operationeel risico niet onnodig te vergroten. Daarnaast mag uitbesteding niet wezenlijk afbreuk doen aan de kwaliteit van haar interne controle en aan het vermogen van de toezichthouder (zowel AFM als DNB) om te controleren of de onderneming alle verplichtingen nakomt. Uit de concept-uitvoeringsrichtlijn volgt dat de beleggingsonderneming in geval van uitbesteding verantwoordelijk blijft voor de uitbestede diensten en voldoende expertise dient te behouden om de uitbestede diensten te kunnen monitoren en de hiermee verwante risico's te kunnen beheersen. Daarnaast dient de beleggingsonderneming

procedures op te stellen om de prestaties te meten van de onderneming die de uitbestede diensten verricht. De uitbesteding moet voorts in een zogenaamd service level agreement worden vastgelegd. Ook vereist de concept-uitvoeringsrichtlijn dat de beleggingsonderneming dient te garanderen dat de toezichthouder in staat wordt gesteld te controleren of de uitbestede diensten worden uitgevoerd overeenkomstig de eisen van de MiFID en de concept-uitvoeringsrichtlijn. In dat kader dient de beleggingsonderneming er onder meer voor in te staan dat de toezichthouder toegang heeft tot het bedrijfspand van de dienstverlener (service provider). Bijzondere eisen worden gesteld aan uitbesteding van het vermogensbeheer aan een partij gevestigd in derde landen, zoals een vergunning- of registratieplicht van de partij in het derde land en een MOU [RB: Memorandum of Understanding] van de toezichthouder van de desbetreffende lidstaat met die van het derde land. Deze eisen komen echter grotendeels overeen met de interpretatieve mededeling [RB: Imu] die de AFM ten aanzien van uitbesteding van activiteiten heeft afgegeven.'

Mijn conclusie is dat – hoewel een vrij uitgebreide lijst met voorwaarden is opgesteld⁶² – de MiFID ten opzichte van de huidige regelgeving geen significante 'verzwaringen' in toezicht op/eisen aan uitbesteding sec gaat stellen. Ook lijkt de MiFID geen 'verzwaring' ten opzichte van de Wft, die op moment van inwerkingtreding van de MiFID van kracht is. Wel moet wederom worden bekeken of op punten aanpassingen in de uitbestedingsovereenkomst moeten worden doorgevoerd.⁶³ De MiFID stelt echter wel significant andere eisen aan het proces van effectenbemiddeling/-advisering/vermogensbeheer. Voor effecten(krediet)instellingen die al outsourcen of van plan zijn dit te gaan doen, is het van cruciaal belang om (de impact van) de MiFID nu al te analyseren; de (service level)eisen aan de dienstverlener(s) zullen immers ook significant gaan veranderen. De eerdergenoemde AFM-brochure is een goed startpunt voor deze analyse.⁶⁴

55. Zie artikel PPPP van de Vijfde Nota van Wijziging bij de Wft.

56. Zie artikel 28, lid 2 Bpr.

57. Wat uiteraard ook gevolgen heeft voor aspecten als monitoring.

58. Het is op dit moment nog niet bekend of en hoe een en ander in het overgangsrecht bij de Wft wordt geregeld.

59. Zie artikel 36, lid 3 Bgfo.

60. AFM brochure 'Markets in Financial Instruments Directive (MiFID)', in het bijzonder p. 13 (<<http://www.afm.nl/marktpartijen/default.ashx?folderid=1098&downloadid=6367>>).

61. De MiFID spreekt slechts over 'operationele taken die van *kritiek belang* [curs. RB] zijn voor een continue en bevredigende dienstverlening aan de cliënten en voor het verrichten van beleggingsactiviteiten op een continue en bevredigende basis'; zie artikel 13, lid 5 MiFID jo. artikel 13 concept-uitvoeringsrichtlijn MiFID.

62. Zie artikel 14 concept-uitvoeringsrichtlijn MiFID.

63. Ook hier geldt mijn eerdere opmerking over het overgangsrecht.

64. Voor een uitgebreider verhandeling over de gevolgen van MiFID en een uiteenzetting van informatiebronnen over MiFID verwijs ik naar J.W. Kaptein en G. Roeleven, 'MiFID vanuit het perspectief van compliance' in *TvCo* 2006-4.

Overigens is CESR (The Committee of European Securities Regulators) momenteel bezig met het uitvoeren van haar 'MiFID level 3 work programme'⁶⁵, waarin ook uitbesteding wordt meegenomen. De planning is om de resultaten met betrekking tot outsourcing in het 3^e of 4^e kwartaal 2006 te publiceren. Het is op het moment van schrijven van dit artikel niet duidelijk of aan de toezichthouder een instemmings-/goedkeuringsrecht wordt toegekend. Ik heb hiervoor in de MiFID en de meest actuele tekst van de daarop gebaseerde uitvoeringsmaatregelen geen aanwijzingen gevonden.

8. Slotoverdenkingen en conclusie

Het wezenlijke van de rol van de compliancefunctie is dat deze zowel een inhoudelijke als een procesbegeleidende rol heeft in de verschillende fasen van het uitbestedingsproces. Ik heb in dit artikel getracht om een raamwerk neer te zetten dat compliance officers kunnen hanteren om deze rollen adequaat in te vullen, met het ultieme doel te borgen dat compliancerisico's rondom uitbesteding ade-

quaat worden beheerst. Ik realiseer me uiteraard dat er een enorme diversiteit aan financiële instellingen bestaat, met daarbinnen een enorme (wellicht nog grotere) diversiteit aan uitbestedingprojecten. Ook verschilt de inrichting en scope van de verschillende risicofuncties (waaronder Compliance) per financiële instelling. Niettemin hoop ik dat iedere compliance officer (elementen uit) dit raamwerk kan gebruiken om zijn/haar betrokkenheid bij uitbestedingprojecten te optimaliseren.

Hoe dan ook, het is van groot belang dat de compliancefunctie in een vroegtijdig stadium betrokken is bij uitbestedingprojecten. Hoe kritischer de scope van het project, hoe groter het belang van deze tijdige betrokkenheid. De compliancefunctie heeft een belangrijke rol in alle fasen van een uitbestedingproject. Het onderstaande schema geeft een samenvatting van de belangrijkste compliancegerelateerde activiteiten per fase:

| Vorbereiding | Assessment | Selectie | Onderhandeling | Contracting | Transitie | Transformatie | Monitoring |
|---|--|--|--|---|-----------------------------------|--|--|
| Presentatie aan (project) management | Uitvoeren van/betrokken bij risicoanalyse | Beoordelen RFI/RFP op compliancegerelateerde onderwerpen | Geven van mening/advies over compliancegerelateerde vragen/opmerkingen vanuit het (commerciële) onderhandelings-team | Geven van mening/advies over compliancegerelateerde vragen/opmerkingen vanuit het (juridische) onderhandelings-team | Monitoren van de overgang 'as-is' | Monitoren van de herinrichting van de uitbestede processen | (Laten) monitoren van compliancegerelateerde bepalingen/service levels, beoordelen van rapportages, opvolgen van verbeteracties, inlichten van toezichthouders in geval van grote issues |
| Contacten met toezichthouders (niet exclusief voor deze fase) | Bewaken opvolging risico-mitigerende maatregelen | Compliance-'score' per dienstverlener | Geven van input op/goedkeuren adviesaanvraag OR ⁶⁶ | Beoordelen compliancegerelateerde bepalingen | | | Analyseren van wijzigingen in regelgeving |
| Opstellen Compliance Chart | | | | Betrokkenheid bij inrichting SMO ⁶⁷ | | | Periodieke meetings met de dienstverlener |

In elke fase van het project is het van groot belang om tijdig afstemming te zoeken met de andere risicofuncties, zoals Internal Audit, (Operational) Risk Management, Juridische Zaken en (IT) Security. Het is ook cruciaal om de betrokkenheid van Compliance adequaat te documenteren. De compliancefunctie moet tot slot proactief inspelen op concrete ontwikkelingen op het gebied van financiële regelgeving (concreet: Wft en MiFID) en de bepalingen over uitbesteding hierin.

65. 'CESR Work Programme on MiFID level 3 Work', CESR, juli 2005, p. 3 en 6 (<<http://www.cesr.eu/index.php?docid=3884>>).

66. Ondernemingsraad.

67. Service Management Organisation.