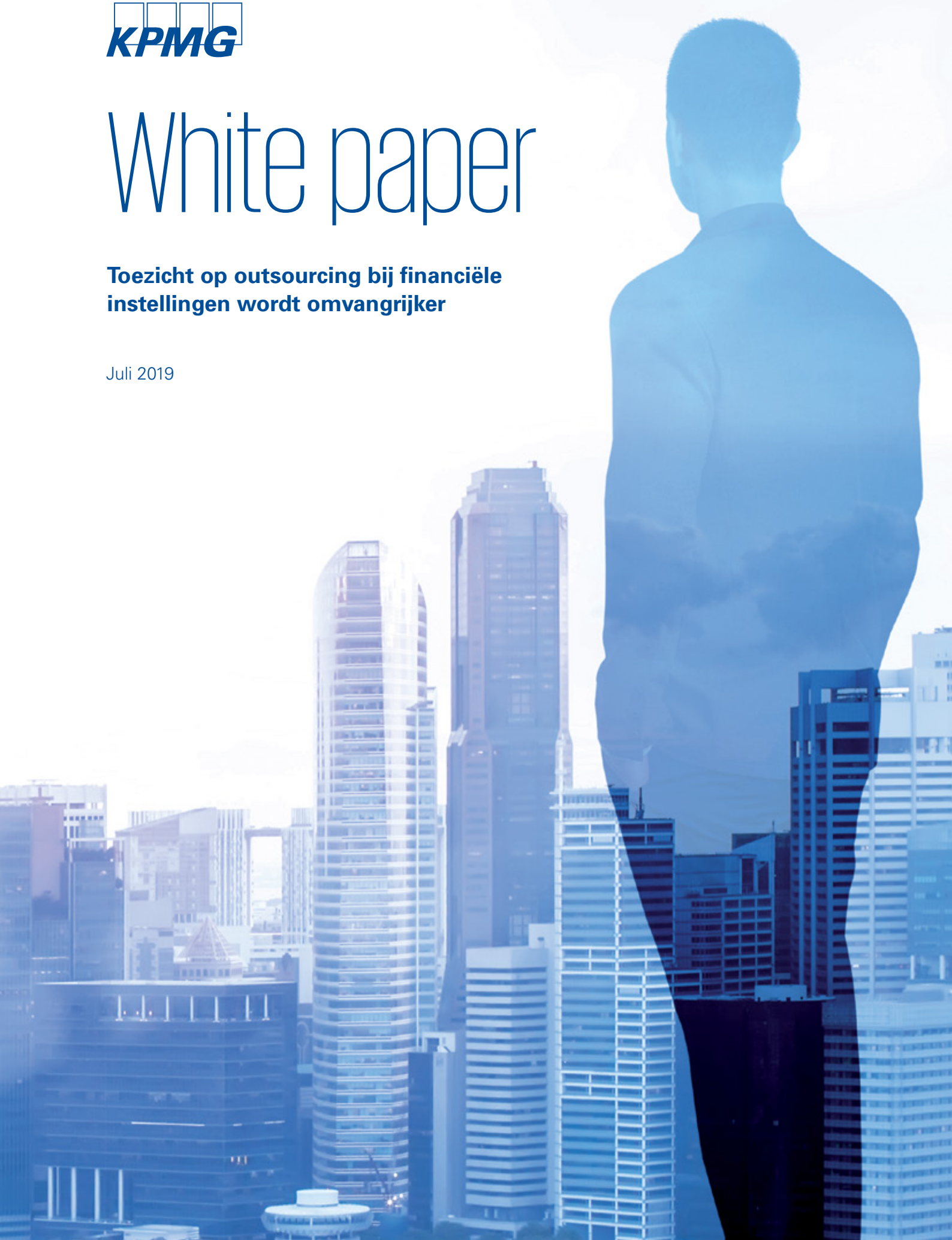
KPMG

# White paper

## Toezicht op outsourcing bij financiële instellingen wordt omvangrijker

Juli 2019



# 1.1 Nieuwe EBA Guidelines voor outsourcing [1]

**De European Banking Authority (EBA) heeft op 25 februari 2019 de finale versie van de 'EBA Guidelines on outsourcing arrangements' (hierna 'Richtlijn') gepubliceerd. De Richtlijn beschrijft de wijze waarop financiële instellingen outsourcingrelaties aangaan, monitoren en beheersen en treedt in werking vanaf 30 september 2019. Alle outsourcingsovereenkomsten die zijn ingegaan op of na deze datum moeten voldoen aan de nieuwe Richtlijn.**

**Voor bestaande outsourcingsovereenkomsten geldt een overgangsregeling, waarbij de overeenkomsten moeten worden aangepast conform de Richtlijn bij de eerstvolgende contractverlengingsmogelijkheid, maar in ieder geval vóór 31 december 2021.**

**Kiruna van Schip**
Manager I Risk & Regulatory FRM

**Maarten Visser**
Manager I Digital Sourcing

### Een allesomvattende outsourcingrichtlijn op Europees niveau

**25 februari 2019**
Final Guidelines gepubliceerd

**30 september 2019**
EBA Guidelines treedt in werking

**31 december 2021**
Einde overgangsregeling bestaande contracten

1 Outsourcing is een overeenkomst van om het even welke vorm tussen een instelling, een betalingsinstelling of een instelling voor elektronisch geld en een dienstverlener op grond waarvan deze dienstverlener een proces, een dienst of een activiteit verricht die anders door de instelling, betalingsinstelling of instelling voor elektronisch geld zelf zou worden verricht. *EBA Richtsnoeren inzake uitbesteding, 25 februari 2019.*

2 Voor toepassing van de nieuwe Richtlijn worden instellingen als gedefinieerd in artikel 3, lid 1, punt 3, van Richtlijn 2013/36/EU op individuele, gesubconsolideerde en geconsolideerde basis aangemerkt. Daarnaast zijn betalingsinstellingen en instellingen voor elektronisch geld op individuele basis aan deze Richtlijn onderhevig. *EBA Richtsnoeren inzake uitbesteding, 25 februari 2019.*

Outsourcing is een bewezen manier om toegang te krijgen tot (technologische) innovaties en schaalvoordelen. Door outsourcing ontstaan echter ook weer nieuwe risico's bij financiële instellingen, derde partijen én toezichthouders. De nieuwe Richtlijn beoogt deze risico's te identificeren, adresseren en mitigeren.

De Committee of European Banking Supervisors (CEBS), de voorganger van de EBA, heeft in 2006 richtlijnen voor outsourcing gepubliceerd. Deze richtlijnen komen te vervallen wanneer de Richtlijn op 30 september 2019 in werking treedt. De nieuwe Richtlijn vervangt tevens de in 2018 gepubliceerde EBA-aanbevelingen voor outsourcing aan cloudserviceproviders. Met de nieuwe Richtlijn introduceert de EBA één allesomvattende outsourcingrichtlijn die als nieuwe norm geldt voor financiële instellingen binnen de EU. Dit sluit aan bij de roep vanuit toezichthoudende instanties voor meer overkoepelende regelgeving in plaats van een complexe verzameling van losstaande en lokale richtlijnen.

| Guideline / Recommendation | Status |
|---|---|
| EBA Guidelines on Outsourcing<br>Jaar van publicatie: 2019 | Geldig vanaf 30 september 2019 |
| EBA Recommendation for Cloud Outsourcing<br>Jaar van publicatie: 2018 | Ingetrokken vanaf 30 september 2019 |
| CEBS Guidelines on Outsourcing<br>Jaar van publicatie: 2006 | Ingetrokken vanaf 30 september 2019 |
| DNB-richtlijnen, onder andere 'Governance bij uitbesteding' en 'Good practices beheersing risico's bij uitbesteding' | Geldig, nog onbekend of deze ingetrokken worden in verband met de nieuwe Richtlijn |

# 1.2 Richtlijn voor outsourcing: de financiële instelling mag geen lege huls worden

**De Richtlijn schrijft voor dat de outsourcingspolicy van financiële instellingen moet aansluiten bij de levenscyclus van outsourcing, waarbij risico's en verantwoordelijkheden per fase worden geadresseerd.**

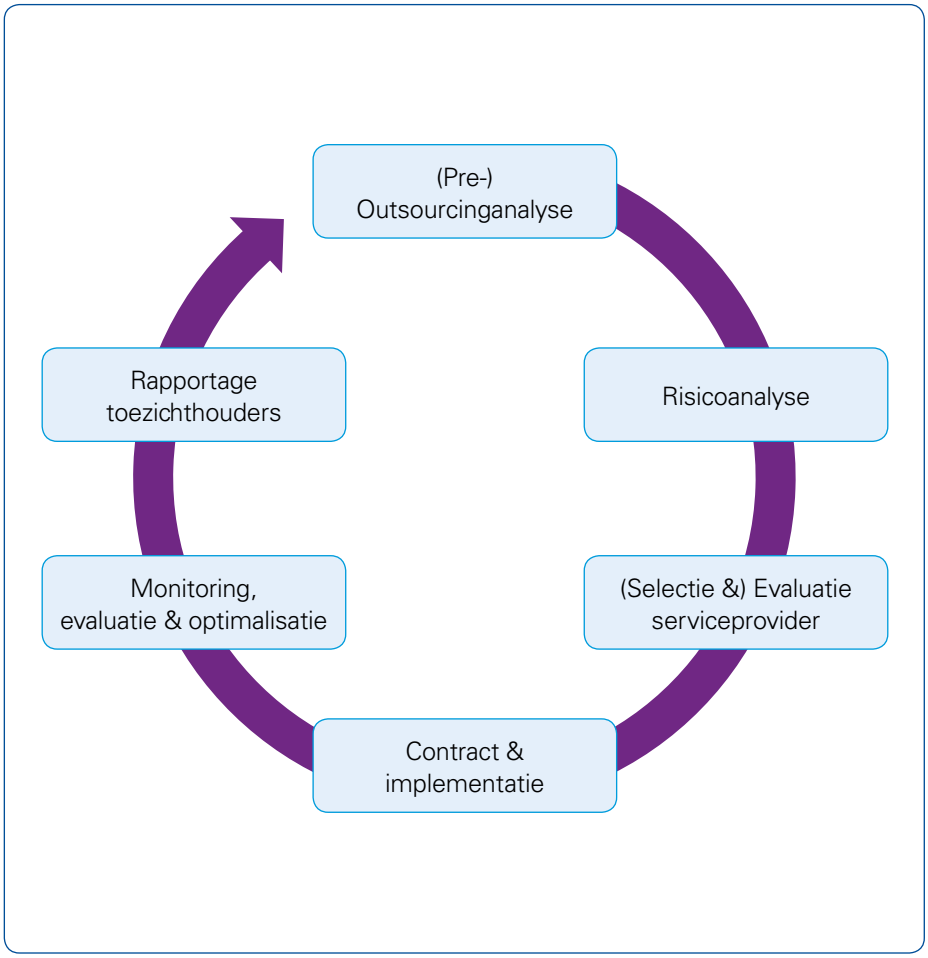
Om de vereisten per fase duidelijk weer te geven is de Richtlijn op hoofdlijnen opgebouwd uit de volgende onderdelen:

**A. Proportionaliteit en groepstoepassing;**

**B. Assessment van outsourcing-overeenkomsten;**

**C. Governance framework; en**

**D. Outsourcing proces.**




Hieronder volgt per onderdeel een beknopte uiteenzetting van de belangrijkste vereisten in de Richtlijn.

## A. Proportionaliteit en groepstoepassing

De Richtlijn is van toepassing op de gehele corporate groep en geldt dus ook voor dochter-bedrijven. Op deze manier wordt een adequate en consistente toepassing van de Richtlijn afgedwongen, ook als dochterondernemingen buiten de EU-grenzen zijn gevestigd.

In de Richtlijn wordt het principe van proportionaliteit benadrukt. Financiële instellingen die bedrijfsactiviteiten willen uitbesteden dienen de aard, schaal en complexiteit van deze activiteiten af te wegen, zodat uitbestedingsrisico's zorgvuldig kunnen worden ingeschat en passende maatregelen kunnen worden doorgevoerd. Dit houdt echter niet in dat de verantwoordelijkheid voor de bedrijfsactiviteiten kan worden overgedragen aan de serviceprovider. Zowel in de Richtlijn als publicaties vanuit toezichthouders wordt het belang benadrukt voor financiële instellingen om verantwoordelijkheid te behouden. Zo licht de EBA specifiek toe dat bepaalde management- taken nooit mogen worden uitbesteed, zoals de bepaling van het risicoprofiel van de financiële instelling en management-besluitvorming.

Ondanks dat de eindverantwoordelijkheid altijd bij het bestuursorgaan blijft liggen, moeten financiële instellingen ervoor waken dat er geen aaneenschakeling van uitbestede activiteiten ontstaat, met slechts behoud van de financiële eindverantwoordelijkheid (een zogenaamde 'lege huls'). Er moet voldoende kennis en ervaring in huis blijven om de continuïteit van de financiële instelling te waarborgen en om effectief toezicht te kunnen houden op de (kwaliteit van de) diensten van de serviceprovider.

## B. (Re-)assessment van outsourcingsovereenkomsten

Allereerst dient te worden bepaald of er sprake is van outsourcing. De Richtlijn schrijft voor dat er sprake is van outsourcing wanneer de uitbesteding van activiteiten een voortdurend of terugkerend karakter kent. Zo wordt een eenmalig advies voor een rechtszaak of de inhuur van een derde partij voor onderhoudswerkzaamheden aan een pand niet als outsourcing bestempeld. De EBA heeft verder een aantal voorbeelden opgenomen in de Richtlijn van activiteiten die niet als outsourcing worden gezien, ongeacht het terugkerende karakter:

- uitbesteding van diensten die anders niet door de financiële instelling zouden worden uitgevoerd. Hierbij valt te denken aan schoonmaakdiensten, catering, en ondersteuning van administratieve taken, zoals postkamer, receptie en secretariaat;
- uitbesteding van diensten die door wet- en regelgeving worden toegewezen aan een derde partij (bijvoorbeeld de externe accountant voor de jaarrekeningcontrole);
- serviceproviders van marktinformatiediensten, zoals Bloomberg en Standard & Poor's;
- clearing- en afwikkelingsactiviteiten bij effectentransacties.

De Richtlijn legt een verantwoordelijkheid bij de financiële instelling om een goede outsourcingspolicy te hebben, waar alle aspecten in detail worden geadresseerd. Zo zijn er extra vereisten voor uitbesteding van kritieke of belangrijke functies en dient er een grondige analyse te worden gemaakt van de outsourcingsrisico's. Bovendien dient er bij intra-groep uitbestedingen sprake te zijn van het 'arm's length principe', wat betekent dat gehandeld moet worden alsof men handelt met een onafhankelijke derde.

In de Richtlijn is er in het bijzonder aandacht voor uitbesteding aan serviceproviders die gevestigd zijn in derdewereldlanden. Elementen die onder andere dienen te worden overwogen hebben betrekking op sociale en ethische verantwoordelijkheid, informatiebeveiliging en privacy, maar ook specifiek op de bevoegdheden van lokale toezichthouders en de zekerheden die dienen te worden gesteld voor effectief toezicht (zoals toegang tot data, documenten, panden en personeel).

## C. Governance framework

De Richtlijn schrijft strikte eisen voor ten aanzien van het governance framework van de financiële instellingen. Een aantal randvoorwaarden zijn als volgt:

- Outsourcing mag nooit leiden tot delegatie of uitbesteding van verantwoordelijkheden van het management van de financiële instelling;
- De verantwoordelijkheden voor de documentatie, het beheer en de controle van outsourcingsovereenkomsten zijn duidelijk vastgelegd in een outsourcingpolicy. Deze policy dient regelmatig te worden beoordeeld en/of herzien;
- Voor outsourcing van kritieke of belangrijke functies geldt dat er Business Continuity en Exit plannen aanwezig moeten zijn, die regelmatig worden getest en herzien waar nodig. Er dient voldoende kennis en ervaring in huis te worden gehouden om te continuïteit van de onderneming te waarborgen en te voorkomend dat de instelling een 'lege huls' wordt;
- De interne audit functie voert een onafhankelijke review uit op de outsourcingovereenkomsten en volgt hierbij een risk-based aanpak. Belangrijk is dat hierbij ook conflicterende belangen worden beoordeeld. Deze dienen door het management te worden geïdentificeerd, beoordeeld en beheerst;
- Er dient een outsourcing register te worden onderhouden met daarin alle informatie over de outsourcingovereenkomsten op groeps- en entiteitniveau. Dit register is noodzakelijk voor een accurate en volledige rapportage over uitbestedingen aan de toezichthoudende instanties.

## D. Outsourcing proces

De Richtlijn beschrijft de vereisten voor het outsourcing proces. Een aantal randvoorwaarden wordt hieronder kort samengevat, waarbij de Richtlijn de outsourcing lifecyle volgt:

- Er dient een pre-outsourcing analyse te worden uitgevoerd voordat een outsourcing overeenkomst wordt aangegaan;
- Voor aanvang van de outsourcing dient de potentiële impact van de outsourcing op het operationele risico beoordeeld te worden, zodat passende maatregelen genomen kunnen worden;
- Alvorens een outsourcingovereenkomst aan te gaan, dient tijdens het selectie- en beoordelingsproces beoordeeld te worden of de dienstverlener geschikt is. Hierbij dient de financiële instelling ook te analyseren waar de diensten worden verleend (bijvoorbeeld binnen of buiten de EU);
- De rechten en plichten van de financiële instelling en de service provider moeten duidelijk worden toegewezen en vastgelegd in een schriftelijke overeenkomst;
- De prestaties van de service provider en outsourcing risico's dienen continu te worden gemonitord voor alle uitbestede diensten, met een focus op belangrijke en kritieke functies. Alle uitbestedingen dienen per medio 2019 aan de toezichthouder te worden gerapporteerd;
- Voor de outsourcing van kritieke en belangrijke functies dient er een duidelijk gedefinieerde exit strategie te zijn in lijn met de outsourcingspolicy en Business Continuity plannen.

# 1.3 Impact op de financiële sector

**De nieuwe Richtlijn raakt niet alleen financiële instellingen, maar ook toezichthouders en serviceproviders. Er is een verregaande impact wanneer de Richtlijn in werking treedt op 30 september, maar de invloed van de nieuwe regelgeving op de outsourcingsactiviteiten en het bijbehorende risico verschilt per betrokkene.**

## 1.3.1 Toezichthouders dienen een nieuwe vorm van concentratierisico te bewaken

Technologische vernieuwing is een van de speerpunten van DNB in de 'Visie op Toezicht 2018-2022'. De analyse van de consequenties en nieuwe risico's van een meer 'open' bankensector voor het prudentiële en integriteitstoezicht staan sterk in relatie tot de publicatie van de nieuwe Richtlijn voor outsourcing.

Naast toezicht op de financiële instellingen, wordt DNB door de nieuwe Richtlijn verantwoordelijk voor het monitoren van het zogenoemde concentratierisico. Dit risico ontstaat wanneer bepaalde bedrijfsactiviteiten door verschillende financiële instellingen worden uitbesteed bij eenzelfde serviceprovider. Dit kan de continuïteit en operationele weerbaarheid van financiële instellingen in het gedrang brengen indien de serviceprovider in (financiële) problemen komt. Aangezien outsourcingsovereenkomsten op dit moment niet, of nog niet volledig, centraal worden geregistreerd is er op dit moment geen volledig beeld.

In 2017 heeft DNB een thematisch onderzoek uitgevoerd bij banken, beleggingsondernemingen en betaalinstellingen naar de omvang en beheersing van het uitbestedingsrisico's. In juni 2018 is hieruit de 'Good practices beheersing risico's bij uitbesteding' voortgekomen, welke onder meer de eis voor financiële instellingen toelicht om outsourcing van materiële activiteiten te melden bij de toezichthouder. Op dit moment onderhoudt DNB een register van alle lopende outsourcingsovereenkomsten aan cloudserviceproviders. Met de nieuwe Richtlijn wordt deze meldplicht medio 2019 verder uitgebreid naar overige uitbestedingen om een volledig beeld te krijgen van (onder)uitbestedingen door financiële instellingen.
Dit stelt de toezichthouder in staat om de concentratie van outsourcing te monitoren en het risico beter te beheersen. Daarnaast stelt het DNB in staat om te monitoren dat er geen financiële instellingen ontstaan waarbij vrijwel alle activiteiten zijn uitbesteed en de instelling zelf niet veel meer is dan een 'lege huls'.

De Richtlijn benadrukt dat financiële instellingen een clausule in de outsourcingspolicy en overeenkomst moeten opnemen welke DNB en andere toezichthoudende instanties het recht geeft om inspecties uit te voeren indien en waar nodig geacht. Hoewel deze clausule al verplicht werd gesteld in eerdere EBA guidelines, blijkt in de praktijk dat de clausule veelal niet is opgenomen in outsourcingsovereenkomsten.

## 1.3.2 Financiële instellingen worden extra gewezen op hun zorgplicht

De nieuwe Richtlijn heeft een grote impact op de financiële instellingen, waarbij op hoofdlijnen een vierdeling kan worden gemaakt van de problematiek en uitdagingen:

**A. Behoud van (eind)verantwoordelijkheid en voorkomen van 'lege huls'**

**B. Operationele weerbaarheid financiële instellingen**

**C. Centrale vastlegging uitbestedingen en managementinformatie**

**D. Toenemende concurrentie voor banken**

### A. Behoud van (eind)verantwoordelijkheid en voorkomen van 'lege huls'

Om de taken en verantwoordelijkheden van zowel de financiële instelling als de serviceprovider vast te leggen, dient de outsourcingspolicy te worden geëvalueerd en waar nodig herzien om aansluiting met de Richtlijn te garanderen. Om de uitbestedingsrisico's effectief te beheersen wordt geadviseerd om één verantwoordelijke (unit, Committee, of CRO) aan te stellen voor het monitoren van het risico en naleving van de regelgeving. Het is daarom ook van belang dat outsourcingsovereenkomsten met de serviceproviders worden beoordeeld en aangepast zodat er aansluiting is met de vereisten in de Richtlijn.

### B. Operationele weerbaarheid financiële instellingen

Met de toenemende interesse voor outsourcing van bedrijfsactiviteiten is er een verschuiving van operationele risico's naar leveranciersrisico's zichtbaar. Het concentratierisico is hierboven al kort beschreven, maar daarnaast ontstaat er ook in toenemende mate het step-in risk dat de financiële instelling zelf (financiële) ondersteuning moet verlenen om de serviceprovider staande te houden wanneer deze partij in (financiële) moeilijkheden verkeert. Dit step-in risk dient ingeschat te worden voor het aangaan van een overeenkomst en dient te worden beheerst gedurende de looptijd van de outsourcing en te worden meegenomen in de ICAAP ('Internal Capital Adequacy Assessment Process').

**C. Centrale vastlegging uitbestedingen en managementinformatie**

Uit analyses, inspecties en onderzoeken van onder andere toezichthoudende instanties is naar voren gekomen dat veel instellingen geen centraal outsourcingsregister hebben en dat de managementinformatie omtrent uitbestedingen veelal summier is. Zo heeft het bestuur vaak onvoldoende inzicht in de omvang van de outsourcing en de relevante risico's. Om aan de meldplicht van DNB te kunnen voldoen, dienen financiële instellingen een eigen outsourcingsregister te creëren en onderhouden. Daarnaast bestaat het risico dat de uitbesteding van activiteiten ten onrechte niet wordt gezien als outsourcing. Als gevolg hiervan wordt de uitbesteding niet opgenomen in het outsourcingsregister en ook niet gerapporteerd aan de toezichthouder. Ook de beoordeling of functies kritiek of belangrijk zijn is enigszins subjectief en kan leiden tot een verkeerde categorisatie met het gevaar dat risico's niet in lijn met de outsourcingspolicy worden geëvalueerd en beheerst.

**D. Toenemende concurrentie voor banken**

Naast de uitbreiding en aanscherping van wet- en regelgeving heeft de bankensector te maken met een toename van nieuwe toetreders zoals FinTech- en BigTech-ondernemingen. Door het toetreden van niet-bancaire instellingen die onder andere betalingsdiensten aanbieden ondervinden banken in toenemende mate concurrentie. Er kan een strategische keuze worden gemaakt om te outsourcen in plaats van zelf te innoveren, waardoor er sneller en efficiënter toegang kan worden verkregen tot (technologische) innovaties.

### 1.3.3 Serviceproviders vallen niet buiten schot: nieuwe vereisten door de Richtlijn

De nieuwe Richtlijn heeft niet alleen een grote impact op financiële instellingen, maar ook op serviceproviders. Hoewel zij niet direct vallen onder de reikwijdte van de Richtlijn, is de verwachting dat financiële instellingen de vereisten zullen opleggen aan serviceproviders om te kunnen voldoen aan de nieuwe Richtlijn. Als gevolg hiervan zullen FinTech-bedrijven en andere toetreders voor de uitdaging komen te staan om innovatief en concurrerend te blijven in een snel veranderende markt, terwijl ze tegelijkertijd geconfronteerd worden met de administratieve uitdagingen van het (indirect) naleven van de Richtlijn. Vooral het implementeren van robuuste beheersprocessen en het voldoen aan (interne) documentatievereisten kunnen een aanzienlijke lastenverzwaring zijn voor opkomende serviceproviders.

## 1.4 Kortom, de nieuwe Richtlijn heeft een verregaande impact

De Richtlijn heeft een verregaande impact op de financiële sector en met name voor banken en hun serviceproviders. Het governance framework van de instellingen dient te worden geëvalueerd en mogelijk herzien op meerdere aspecten om naleving van de nieuwe regelgeving te waarborgen. Daarnaast wordt het met de toename van uitbestedingen steeds belangrijker dat financiële instellingen een goede interne beheersing hebben. Hierbij spelen ingebouwde controles een belangrijke rol, zoals het 'three lines of defence'-model waarbij functiescheiding en monitoring door onafhankelijke afdelingen worden nageleefd. Het aanpassen van het governance framework, de outsourcingspolicy, processen, outsourcingsovereenkomsten en dergelijke kost veel tijd en dient grondig, maar vooral ook tijdig, te gebeuren om sancties van toezichthoudende instanties te voorkomen.

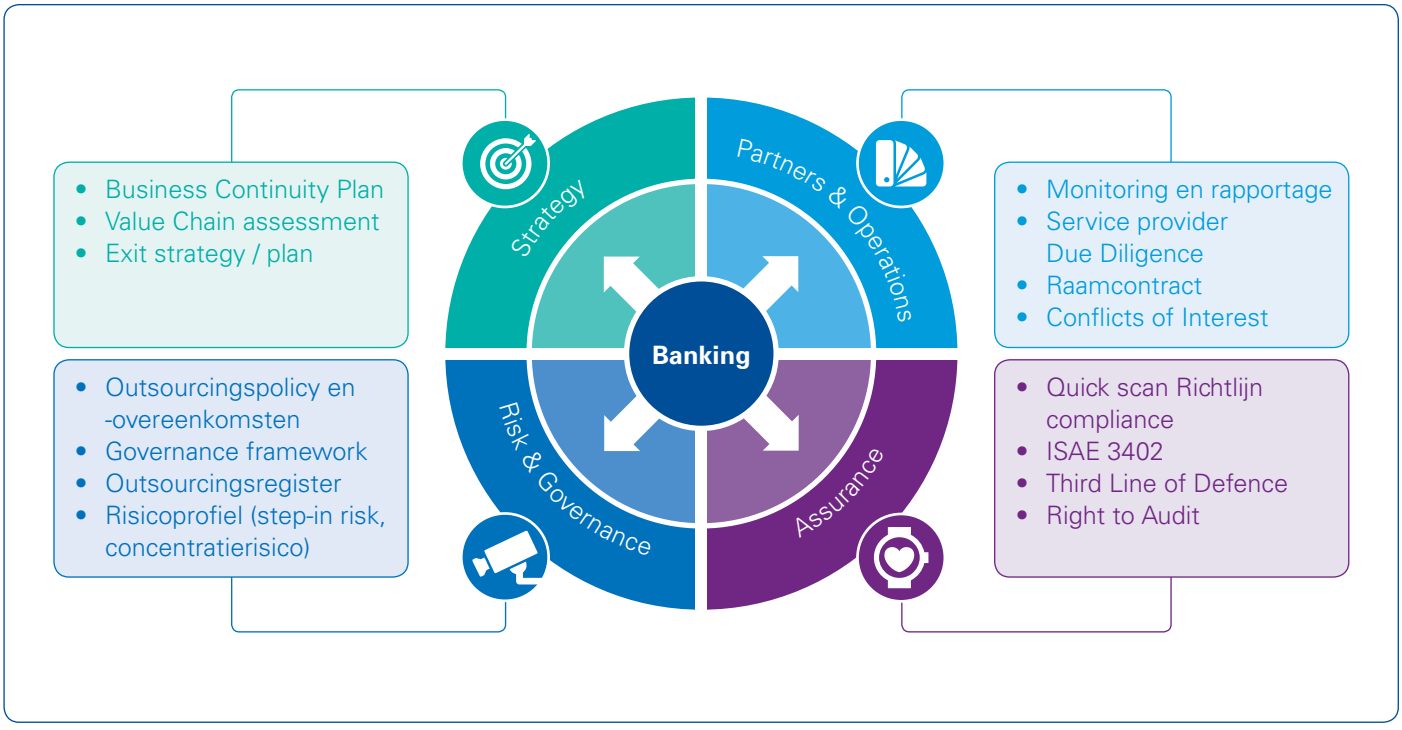
# 1.5 Vervolgstappen

De Richtlijn treedt in werking op 30 september 2019. Het is daarom van belang dat financiële instellingen én serviceproviders een gedetailleerde review uitvoeren op onder andere de outsourcingspolicy en -overeenkomsten en deze waar nodig herzien om te voldoen aan de nieuwe Richtlijn.

We zien in de praktijk dat financiële instellingen de gedetailleerde review vaak onderschatten en dat de benodigde aanpassingen voor voldoen aan de Richtlijn complexer blijken dan in eerste instantie gedacht. Het reviewen en aanpassen van de outsourcingspolicy kan vaak niet zonder een update van de governance policy, waardoor het risico ontstaat dat onderdelen over het hoofd worden gezien en er inconsistenties optreden tussen de verschillende documenten. Het is daarom van belang dat instellingen een tijdige en grondige review uitvoeren om uitdagingen door tijdsdruk en complexiteit te voorkomen.

Daarnaast willen wij benadrukken dat financiële instellingen ervoor moeten waken om een 'lege huls' te worden door de toenemende mate van outsourcing. Zoals beschreven dient de instelling eindverantwoordelijkheid te behouden. Door de nieuwe Richtlijn zal er hernieuwde aandacht van toezichthouders zijn voor dit onderdeel, met mogelijk verregaande consequenties indien niet meer aan de voorwaarden van de licenties wordt voldaan.

KPMG kan assisteren bij iedere fase van de levenscyclus van outsourcing. Ons team heeft de juiste kennis, ervaring én sectorkennis om te helpen bij een gedetailleerde risicoanalyse en de aanpak voor een effectieve beheersing van outsourcingrisico's. Het KPMG-controleframework verzekert u ervan dat alle aspecten van de Richtlijn in overweging worden genomen en waarborgt dat u de vereisten van de nieuwe regelgeving naleeft.



# Vragen?

**Hebt u naar aanleiding van dit artikel vragen over de Richtlijn en outsourcing, dan kunt u contact opnemen met ons team.**


**Kees Stigter**
Partner Digital Sourcing
**T** +31 (0) 30 658 30 39
**E** Stigter.Kees@kpmg.nl

**Gertjan Thomassen**
Partner Risk & Regulatory FRM
**T** +31 (0) 20 656 79 62
**E** Thomassen.Gertjan@kpmg.nl

**Paul Rothwell**
Partner Finance FS
**T** +31 (0) 20 656 44 42
**E** Rothwell.Paul@kpmg.nl

**Mark van Vugt**
Senior Manager Risk & Regulatory FRM
**T** +31 (0) 20 656 78 76
**E** vanVugt.Mark@kpmg.nl