Beheerst uitbesteden

Verkenning naar uitbestedingsrisico’s bij financieel dienstverleners

Publicatiedatum: 28 juni 2021
Classificatie: AFM - Publiek

Autoriteit Financiële Markten

De AFM maakt zich sterk voor eerlijke en transparante financiële markten.

Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.

Inhoudsopgave

1. Inleiding

In de tweede helft van 2020 heeft de AFM onder financieel dienstverleners een uitvraag naar uitbesteding uitgevoerd. Het doel ervan was om inzicht te krijgen in welke uitbestedingsrisico's, waar en in welke mate voorkomen en de mate waarin en wijze waarop deze risico's worden beheerst door financieel dienstverleners. Met dit inzicht kan de AFM zorg dragen voor proactief en risicogestuurd toezicht op uitbesteding. In deze sectorbrede terugkoppeling geeft de AFM de belangrijkste resultaten van de verkenning weer. Daarnaast heeft de AFM good practices geformuleerd voor het beheersen van uitbestedingsrisico's.

De AFM heeft voor de uitvraag uitbesteding 246 middelgrote en grote financieel dienstverleners benaderd. Het gaat dan om zowel adviseurs & bemiddelaars als kredietaanbieders die over een vergunning van de AFM beschikken. Aan de geselecteerde financieel dienstverleners is gevraagd om alle belangrijke of kritieke activiteiten te melden die zijn uitbesteed aan externe partijen of binnen de groep waarvan de financieel dienstverlener onderdeel uitmaakt (intragroep uitbesteding). Een uitbesteding is belangrijk of kritiek indien het tijdelijk of permanent uitvallen van de onderliggende activiteit leidt tot ongewenste juridische, operationele en/of financiële risico's voor de onderneming en de klanten van uw onderneming. Vanwege toenemende digitalisering en het steeds vaker uitbesteden van kritische en belangrijke ICT-diensten is het ook in het belang van de financiële consument en het vertrouwen in de financiële dienstverlening dat de toenemende risico's gerelateerd aan uitbesteding worden gemitigeerd. De deelnemende financieel dienstverleners hebben in totaal 1081 uitbestedingen gemeld. Meer dan de helft van de gemelde uitbestedingen had betrekking op ICT. Ondernemingen waar activiteiten naartoe zijn uitbesteed, zullen in dit rapport worden aangeduid als serviceprovider.

De resultaten van de uitvraag over de beheersing van uitbesteding zijn vergelijkbaar voor adviseurs & bemiddelaars en voor kredietaanbieders. In dit rapport wordt daarom geen onderscheid gemaakt tussen deze twee populaties.

Hoofdstuk 2 schetst een marktbeeld van uitbesteding door financieel dienstverleners. In hoofdstuk 3 formuleert de AFM aandachtspunten op basis van good practices voor het beheersen van uitbestedingsrisico's en verwachtingen om te voldoen aan de wettelijke eis voor incidentmeldingen aan de AFM. De AFM verwacht dat financieel dienstverleners kennisnemen van deze good practices en deze gebruiken om risico's met betrekking tot uitbesteding te verkleinen. Bijlage A geeft een overzicht van het relevante wettelijk kader. In bijlage B worden gedetailleerde resultaten van de uitvraag weergegeven.

2. Marktbeeld uitbestedingen door financieel dienstverleners

Dit hoofdstuk schetst een algemeen marktbeeld van de uitbesteding door financieel dienstverleners, zoals blijkt uit de antwoorden op de uitvraag. Hierbij wordt beoordeeld in welke mate er sprake is van concentratie van uitbestedingen naar een paar serviceproviders. Ook wordt een overzicht gegeven van type uitbestedingen en het vestigingsland van de serviceprovider. Meer gedetailleerde statistische resultaten van de uitvraag worden weergegeven in bijlage B.

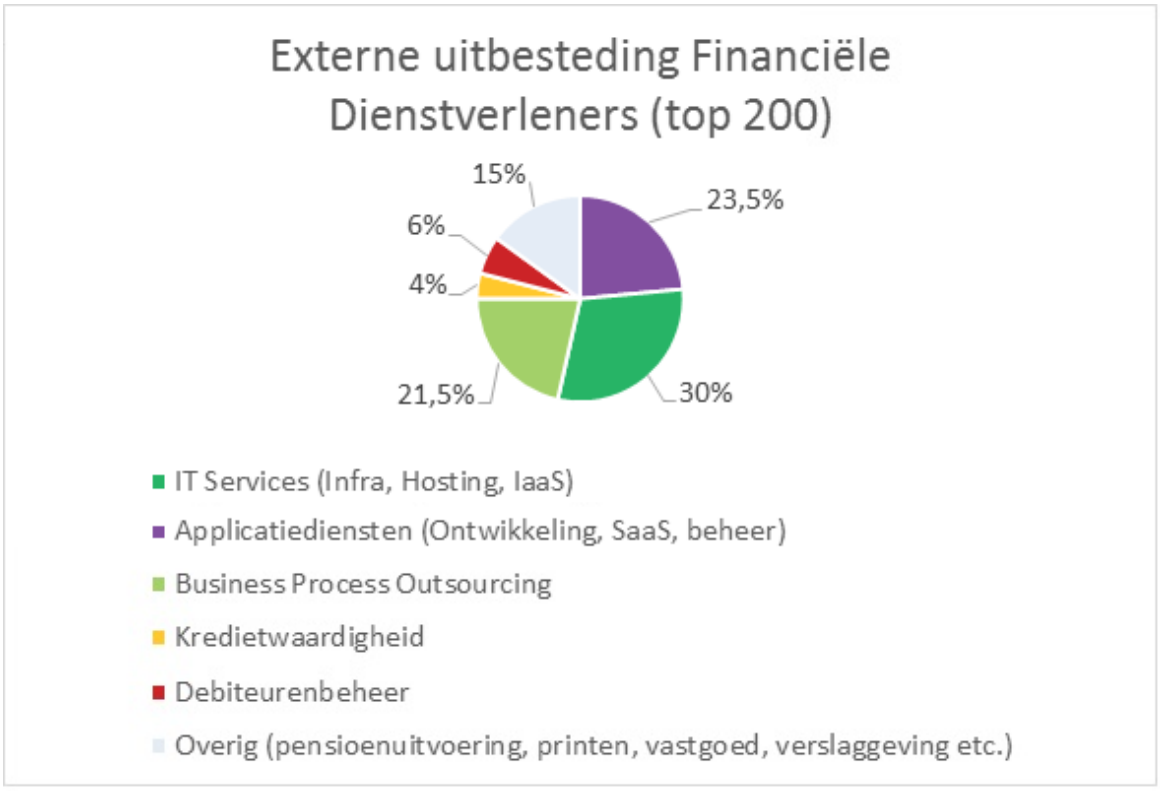
Marktconcentratie is beperkt. Indien veel financieel dienstverleners gebruikmaken van dezelfde serviceprovider, kunnen er concentratierisico's ontstaan. Een continuïteitsprobleem bij de serviceprovider kan in dit geval een grote impact hebben op de financiële sector als geheel. Uit de resultaten komt weinig marktconcentratie naar voren binnen de onderzochte populatie. Zes serviceproviders verlenen diensten aan meer dan tien van de deelnemende financieel dienstverleners. Bij deze zes serviceproviders kan sprake zijn van concentratierisico's. Daarnaast leverden 78% van de IT-serviceproviders slechts aan één of twee van de deelnemende financieel dienstverleners diensten.

De AFM constateert daarnaast dat financieel dienstverleners weinig uitbesteden aan de grote cloud service providers[1] en dat ook hier geen sprake is van grote concentratie. Bij minder dan 1% van de uitbestedingen onder financieel dienstverleners is sprake van uitbesteding naar cloud service providers, zoals Amazon, Microsoft of Google. Wel ziet de AFM dat gebruik wordt gemaakt van enkele lokale cloud service providers.

Er wordt vooral uitbesteed naar Nederlandse serviceproviders. De meeste serviceproviders zijn in Nederland gevestigd: 91% van de serviceproviders heeft een vestigingsadres in Nederland. Hierbij heeft de AFM niet onderzocht of deze serviceproviders alleen administratief in Nederland gevestigd zijn en hun daadwerkelijke activiteiten van buiten Nederland uitvoeren of dat ze daadwerkelijk vanuit Nederland hun bedrijfsvoering uitoefenen. 96% van de uitbestedingen vinden plaats door serviceproviders in de EU en 4% buiten de EU.

Het merendeel van de uitbestedingen betreft ICT. Meer dan 50% van de uitbestedingen zijn ICT gerelateerd, zoals applicatiebeheer, beheer van infrastructuur, hosting, netwerkdiensten en software as a service. Daarnaast worden ook in veel gevallen bedrijfsprocessen uitbesteed. Dit betreft veelvuldig debiteurenbeheer. Een classificatie van de 200 grootste externe uitbestedingen op basis van de jaarlijkse contractwaarde is weergegeven in de figuur hieronder.

[1] Onder clouduitbesteding wordt verstaan: uitbestedingen geleverd met behulp van cloud computing, dat wil zeggen: een model voor het snel beschikbaar stellen van on-demand netwerktoegang tot een gedeelde pool van configureerbare IT-middelen zoals netwerken, servers, opslag, applicaties en diensten, die met een minimum aan managementinspanning of interactie met de dienstverlener beschikbaar kunnen worden gesteld. (Bron: NIST)


Externe uitbesteding Financiële Dienstverleners (top 200)
15%
23,5%
6%
4%
21,5%
30%
IT Services (Infra, Hosting, IaaS)
Applicatiediensten (Ontwikkeling, SaaS, beheer)
Business Process Outsourcing
Kredietwaardigheid
Debiteurenbeheer
Overig (pensioenuitvoering, printen, vastgoed, verslaggeving etc.)

3. Aandachtspunten voor het verbeteren van de interne beheersing van uitbestede activiteiten

Financieel dienstverleners blijven verantwoordelijk voor de kwaliteit van de uitbestede diensten en activiteiten. Echter, het uitbesteden van kritische of belangrijke activiteiten brengt ook risico's met zich mee. Door het implementeren van interne beheersmaatregelen kunnen deze risico's worden teruggebracht tot een acceptabel niveau. De AFM heeft deze verkenning gebruikt om inzicht te krijgen in de interne beheersing van uitbesteding bij financieel dienstverleners. De belangrijkste bevindingen worden in dit hoofdstuk beschreven. Ook heeft de AFM aandachtspunten op basis van good practices geformuleerd om risico's met betrekking tot uitbesteding te verkleinen. De AFM verwacht dat financieel dienstverleners kennisnemen van deze good practices en gebruiken om uitbestedingsrisico's tot een acceptabel niveau terug te brengen. Daarnaast verwacht de AFM dat financieel dienstverleners voldoen aan de wettelijke meldplicht voor het melden van incidenten aan de AFM. Deze meldplicht geldt ook indien het incident zich voordoet bij een serviceprovider.

Maak duidelijke afspraken met de serviceprovider over de omgang met incidenten, zodat direct actie kan worden ondernomen naar aanleiding van een incident en om te voldoen aan de wettelijke eisen rond incidenten en de incidentmeldingsplicht bij de AFM. In bijna 5% van de uitbestedingen worden service levels niet gemonitord door de financieel dienstverlener. Hierdoor bestaat het risico dat de financieel dienstverlener niet op de hoogte is van incidenten bij de serviceprovider, terwijl er wettelijke verplichtingen zijn voor financieel dienstverleners ten aanzien van het beheersen en melden van incidenten. De AFM heeft daarnaast in de beantwoording van de uitvraag 27 incidenten aangetroffen. Hoewel de AFM deze incidenten niet individueel onderzocht heeft, valt het op dat geen enkele van deze incidenten gemeld is bij de AFM ondanks de wettelijke meldingsplicht voor incidenten.

Maak duidelijke afspraken met de serviceprovider over de verantwoordelijkheden en verplichtingen van beide partijen, leg deze schriftelijk vast in een contract en laat beide partijen het contract tekenen. Bij externe uitbestedingen is er in 11% van de uitbestedingsrelaties geen sprake van een getekend contract. Bij intragroep uitbestedingen gaat het om 37% van de uitbestedingen. Indien er geen duidelijke afspraken zijn gemaakt tussen de financieel dienstverlener en serviceprovider over de dienstverlening, bestaat er een verhoogd risico dat de kwaliteit van de geleverde diensten door de serviceprovider uiteindelijk niet voldoet aan verwachtingen. Indien er geen contract is opgesteld en deze niet ondertekend is door beide partijen, wordt daarnaast ook de juridische positie bij eventuele geschillen zwakker.

Analyseer risico's zowel voor het aangaan van een uitbesteding als gedurende de uitbesteding regelmatig en neem de benodigde maatregelen om de risico's tot een aanvaardbaar niveau terug te brengen. Uit de resultaten van de uitvraag blijkt dat er bij 70% van de uitbestedingen geen risicoanalyse is uitgevoerd. Hierbij is er weinig verschil tussen intragroep en externe uitbesteding. Ook is er geen verband tussen de grootte van het risico van de uitbesteding en de mate waarin risicoanalyses worden uitgevoerd. Bij uitbestedingen met een hoog risico waren ook vaak geen risicoanalyses aanwezig. Het uitbesteden van kritieke en belangrijke activiteiten kan bedrijfsrisico's met zich mee brengen. Een risicoanalyse heeft als doel om uitbestedingsrisico's in kaart te brengen. Op basis van de risicoanalyse kunnen beheersmaatregelen genomen worden om deze risico's te beheersen.

Bij een risicoanalyse moet worden gekeken naar zowel het risicoprofiel van de serviceprovider als de aard van de dienstverlening die de serviceprovider levert. Bij de risicoanalyse moeten in ieder geval de volgende risico's meegenomen worden:

- Het risico dat er een te grote afhankelijkheid ontstaat van de serviceprovider, waardoor het moeilijk wordt om over te stappen naar een ander serviceprovider.
- Het risico dat er onvoldoende kennis en personeel aanwezig is bij de financieel dienstverlener om leveranciersselectie, implementatie van de uitbesteding en monitoring van de uitbesteding adequaat uit te voeren.
- Het risico dat de onderneming niet compliant is aan wet- en regelgeving omdat de serviceprovider niet voldoet aan wet- en regelgeving.
- Het risico dat de serviceprovider niet voldoet aan de gemaakte afspraken vanuit zowel kwantitatief (b.v. servicelevels) als kwalitatief (b.v. assurance) perspectief.
- Het risico dat er gegevens gestolen worden of dat de dienstverlening wordt verstoord door cyberaanvallen.

4. Conclusies

Op basis van deze verkenning concludeert de AFM dat financieel dienstverleners kritieke en belangrijke activiteiten gemiddeld uitbesteden naar meer dan vier verschillende serviceproviders. Uitbesteding kan onacceptabele risico's met zich meebrengen voor de onderneming en ook voor de klanten van de onderneming, indien deze risico's niet in voldoende mate worden beheerst. Op basis van de uitvraag heeft de AFM een aantal zwakheden vastgesteld in de beheersing van uitbestedingsrisico's. Op basis hiervan heeft de AFM de volgende aandachtspunten op basis van good practices geformuleerd:

- Maak duidelijke afspraken met de serviceprovider over de omgang met incidenten, zodat direct actie kan worden ondernomen naar aanleiding van een incident en om te voldoen aan de wettelijke eisen rond incidenten en de incidentmeldingsplicht bij de AFM.
- Maak duidelijke afspraken met de serviceprovider over de verantwoordelijkheden en verplichtingen van beide partijen, leg deze schriftelijk vast in een contract en laat beide partijen het contract tekenen.
- Analyseer risico's zowel voor het aangaan van een uitbesteding als gedurende de uitbesteding regelmatig en neem de benodigde maatregelen om de risico's tot een aanvaardbaar niveau terug te brengen.

De AFM verwacht dat financieel dienstverleners kennisnemen van deze good practices en gebruiken om risico's met betrekking tot uitbesteding voor de onderneming en de klant tot een aanvaardbaar niveau terug te brengen.

Daarnaast verwacht de AFM dat financieel dienstverleners voldoen aan de wettelijke meldplicht voor het melden van incidenten aan de AFM. Deze meldplicht geldt ook indien het incident zich voordoet bij een serviceprovider.

Bijlage A: Wettelijk kader

De AFM hanteert voor uitbesteding de definitie van uitbesteden zoals opgenomen in artikel 1:1 van 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;'

Daarnaast stelt artikel 4:15, eerste lid, Wft eisen voor de financieel dienstverlener met betrekking tot het waarborgen van een integere en beheerste bedrijfsvoering. Hieronder valt onder meer dat een financieel dienstverlener zorgdraagt voor de beheersing van de risico's van uitbesteding van activiteiten en diensten. De AFM wijst er verder op dat financiële ondernemingen bij uitbesteding zelf verantwoordelijk blijven voor de kwaliteit van de uitbestede processen. Hieronder valt ook dat financieel dienstverleners erop toezien dat een serviceprovider zich houdt aan de verplichtingen van de financieel dienstverlener die voortvloeien uit wet- en regelgeving, waaronder de Wft, maar ook bijvoorbeeld de Algemene Verordening Gegevensverwerking waar het gaat om de verwerking van persoonsgegevens.

Daarnaast zijn financieel dienstverleners verplicht uit hoofde van hun integere bedrijfsvoering om informatie over incidenten aan de Autoriteit Financiële Markten te verstrekken, zoals beschreven in artikel 4:11, vierde lid van de Wft. De wettelijk eisen aan ernstige incidenten zijn nader uitgewerkt in artikel 29 van het Besluit Gedragstoezicht financiële ondernemingen Wft en stellen dat een financieel dienstverlener:

1) Procedures en maatregelen vaststelt met betrekking tot de omgang met en vastlegging van incidenten;
2) Passende maatregelen neemt als een incident zich voordoet. Deze maatregelen zijn gericht op het beheersen van de opgetreden risico's en het voorkomen van herhaling;
3) De Autoriteit Financiële Markten onverwijld informeert omtrent incidenten.

Hierbij is op basis van artikel 1 Besluit Gedragstoezicht financiële ondernemingen Wft een incident gedefinieerd als "een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van een financiële onderneming". Ook bij serviceproviders komen incidenten voor, die leiden tot een ernstige bedreiging voor de integere bedrijfsvoering van de financieel dienstverlener, zoals bijvoorbeeld storingen aan IT-systemen of cyberaanvallen. Ook voor deze gevallen dient een financieel dienstverlener procedures en maatregelen vast te stellen over hoe zij omgaan met deze incidenten en dient de financieel dienstverlener maatregelen te nemen om de risico's van een incident te beheersen en herhaling te voorkomen en om het incident onverwijld te melden bij de AFM.

Bijlage B: Overzicht resultaten van de uitvraag

In de tabel hieronder worden overige resultaten van de uitvraag weergegeven. Hierbij is geen onderscheid gemaakt tussen externe uitbesteding en intragroep uitbesteding.

Onderwerp uitvraag	Percentage
Ondernemingen met uitbesteding	80,4%
IT is onderdeel van de uitbesteding	65,7%
Er is een alternatieve serviceprovider beschikbaar	87,1%
Gegevensverwerking is onderdeel van de uitbesteding	70,8%
Gegevensopslag is onderdeel van de uitbesteding	77,4%
Er is een risicoanalyse uitgevoerd	29,7%
Uitbestedingen zonder getekend contract	16,2%
Een getekend contract bevat een exit clausule	73,4%
In een getekend contract is auditrecht voor de onderneming opgenomen	48,6%
In een getekend contract is auditrecht voor externe accountants en/of toezichthouders opgenomen	42,8%
In een getekend contract zijn afspraken over onderuitbesteding opgenomen	49,0%
In een getekend contract is opgenomen de serviceprovider jaarlijks een third party assurance type 2 verklaring overlegt	14,0%
Performance indicatoren zijn opgenomen in een getekend contract	12,1%

Autoriteit Financiële Markten
T 020 797 2000 | F 020 797 3800
Postbus 11723 | 1001 GS Amsterdam
www.afm.nl