TOEZICHT RAPPORT

AFM deelt aanbevelingen over uitbestedingsmonitoring

In het kort De Autoriteit Financiële Markten (AFM) heeft onderzoek gedaan in de asset management sector en constateert dat de monitoring op uitbesteding op een aantal punten verbeterd kan worden. De AFM geeft aanbevelingen die zien op de kwalificatie, de inrichting, de monitoringsactiviteiten zelf en de monitoring in geval van uitbesteding binnen een groep en uitbesteding van ICT. De AFM verwacht dat ondernemingen de aanbevelingen in dit rapport meenemen bij de doorlopende beheersing van uitbesteding.

Management samenvatting

Beheerders en beleggingsondernemingen besteden steeds meer van hun werkzaamheden uit. Uitbesteding kan bijdragen aan de efficiëntie en kwaliteit van de bedrijfsvoering, maar brengt ook risico's met zich mee.

De Autoriteit Financiële Markten (**AFM**) heeft daarom de afgelopen jaren onderzoeken uitgevoerd bij beleggingsondernemingen, beheerders van beleggingsinstellingen en beheerders van icbe's naar uitbesteding in de asset management sector in brede zin. De AFM heeft hiermee een beeld gekregen van de materiële werkzaamheden die worden uitgevoerd door derde partijen en de beheersmaatregelen die ondernemingen daarbij treffen ('Keten In Beeld').

In 2023 is de AFM een nieuw onderzoek naar uitbestedingen gestart. Het doel van het onderzoek was het vaststellen van in hoeverre beleggingsondernemingen, beheerders van beleggingsinstellingen en beheerders van icbe's invulling geven aan de op hen van toepassing zijnde wet- en regelgeving met betrekking tot de doorlopende beheersing van uitbestedingsrisico's. Dit rapport bevat een terugkoppeling van de bevindingen van het onderzoek en geeft aanbevelingen ten aanzien van het beheersen van uitbestedingsrisico's.

Het onderzoek was gericht op de doorlopende beheersing van uitbestedingsrisico's. Deze beheersing vindt vooral plaats gedurende de monitoring van bestaande uitbestedingsrelaties, maar begint al eerder in het proces. Essentieel voor de beheersing is het kwalificeren van de uitbesteding en de inrichting van de uitbestedingsrelatie, waaronder het maken van afspraken met de dienstverlener en het vaststellen van welke beheersmaatregelen nodig zijn.

Dit rapport bevat daarom aanbevelingen voor de kwalificatie, de inrichting en de monitoring van uitbestedingen in de asset management sector.

De belangrijkste bevindingen zijn:

1. Ondernemingen hebben niet altijd een goed onderbouwde aanpak ten aanzien van het bepalen van wat gezien moet worden als uitbesteding en welke uitbesteding kwalificeert als materieel.
2. Bij de inrichting van uitbestedingen denken ondernemingen vaak nog te beperkt na over maatregelen en afspraken die voorsorteren op een passende monitoring.
3. Ondernemingen gaan zeer verschillend om met de monitoring van uitbestedingen; een meer consistente en uitlegbare aanpak op grond van risico's is noodzakelijk.
4. Voor intra-groep uitbestedingen wordt vaak (te) veel geleund op informele maatregelen en afspraken.
5. Ondernemingen zijn zich niet altijd bewust van ICT-componenten in uitbestedingen en de bijbehorende ICT-risico's.

SEPTEMBER 2024

AFM

Op grond het onderzoek en de bevindingen heeft de AFM een aantal aanbevelingen voor ondernemingen. Een overzicht van deze aanbevelingen is opgenomen in Bijlage I. Niet alle aanbevelingen zijn voor iedere onderneming even relevant. Sommige aanbevelingen zijn bijvoorbeeld meer relevant voor ondernemingen van een bepaalde omvang of voor bepaalde' type werkzaamheden.

De aanbevelingen zijn bedoeld om meer richting te geven aan wettelijke verplichtingen. Ze zijn niet bedoeld als een uitputtende checklist om te voldoen aan wet- en regelgeving over uitbesteding, maar moeten worden gelezen in samenhang met bestaande wet- en regelgeving en richtlijnen over uitbesteding.

De AFM heeft in het onderzoek ook specifiek gekeken naar ICT-uitbestedingen. Deze vallen op dit moment meestal al onder de uitbestedingsregels. De aanbevelingen in dit rapport zijn daarmee in de meeste gevallen ook relevant voor ICT-uitbestedingen.

De AFM doet in dit rapport geen specifieke aanbevelingen ten aanzien van het beheersen van ICT-risico's bij uitbesteding. Op 17 januari 2025 dienen financiële ondernemingen aan DORA (Digital Operational Resilience Act, (EU) 2022/2554) te voldoen, waarmee er een specifiek wettelijk kader is geïntroduceerd voor ICT-diensten van derde partijen. We verwachten dat de ondernemingen reeds aan de slag zijn met het implementeren van de DORA vereisten. Wel heeft de AFM een aantal observaties over ICT-uitbestedingen opgenomen in het rapport.

Hoofdstuk 1 van het rapport bevat een introductie, met daarin verdere informatie over het onderzoek van de AFM, het juridisch kader en een uitbestedingscyclus aan de hand waarvan de AFM de focus van het onderzoek uitlegt. Hoofdstuk 2 van het rapport bevat een overzicht van de bevindingen die de AFM op basis van het onderzoek heeft vastgesteld. Aan de hand van deze bevindingen heeft de AFM in Hoofdstuk 3 van dit rapport aanbevelingen opgenomen, met per aanbeveling een toelichting. ICT-uitbestedingen worden in een apart hoofdstuk benoemd waarbij de AFM een aantal observaties meegeeft. Tot slot bevat Hoofdstuk 4 van het rapport een afsluiting.

Inhoudsopgave

TOEZICHT RAPPORT

AFM

1. Introductie

1.1 Inleiding

Financiële ondernemingen besteden in toenemende mate uit. Deze ontwikkeling doet zich ook voor bij beleggingsondernemingen, beheerders van beleggingsinstellingen en beheerders van icbe's, hierna 'ondernemingen'. Uitbesteding kan de efficiëntie en kwaliteit van de bedrijfsvoering verhogen, maar brengt ook specifieke risico's met zich mee. De AFM heeft uitbesteding daarom al meerdere jaren als een prioriteit in het toezicht aangewezen.

De AFM heeft in 2018 en 2020 de Keten in Beeld onderzoeken uitgevoerd. Hierbij is vooral gekeken naar de opzet van uitbestedingen, gericht op het vaststellen van wat ondernemingen uitbesteden, aan welke dienstverleners, en of ondernemingen beschikken over schriftelijk beleid en procedures. Bevindingen uit deze onderzoeken zijn door middel van brieven met de sector gedeeld. Deze sectorbrieven bevatten observaties en aandachtspunten die nog steeds relevant zijn voor de beheersing van uitbestedingsrisico's. Zie de Sectorbrief 28 november 2019 en Sectorbrief 21 juli 2021

In 2023 is de AFM een nieuw onderzoek naar uitbestedingen in de asset management sector gestart[1]. Het doel van het onderzoek was het vaststellen van in hoeverre ondernemingen invulling geven aan de op hen van toepassing zijnde wet- en regelgeving met betrekking tot de doorlopende beheersing van uitbestedingsrisico's. Dit rapport bevat een terugkoppeling van de bevindingen van het onderzoek en geeft aanbevelingen ten aanzien van het beheersen van uitbestedingsrisico's.

1.2 De cyclus van uitbesteding en de focus van het onderzoek

Bij de beheersing van uitbesteding valt een aantal fases en activiteiten te onderscheiden. Deze worden in de markt en literatuur op verschillende manieren weergegeven. Onderstaande uitbestedingscyclus vatten deze fases en activiteiten voor dit rapport samen.

Beleid en Governance
In de uitbestedingscyclus staat de organisatorische inrichting die de beheerste bedrijfsvoering faciliteert centraal. Hieronder valt onder andere schriftelijk beleid en procedures en een goede governance structuur. Onderdeel hiervan is tevens de visie van een onderneming op uitbesteding en hoe zij uitbestedingen kwalificeert.

Fase 1. De selectie van een uitbestedingspartner.
De eerste fase van een specifieke uitbestedingsrelatie bestaat onder andere uit het volgen van het besluitvormingsproces rondom het uitbesteden van werkzaamheden, het daaropvolgende selectieproces en het due diligence onderzoek bij geselecteerde ondernemingen. Hierna volgt het afronden van de analyse van de objectieve redenen om de uitbestedingsrelatie, inclusief de Cost Benefit Analyse (CBA).

Fase 2. De inrichting van de uitbestedingsrelatie.
Onder deze fase valt het vormgeven van de relatie met de dienstverlener op basis van de reikwijdte van de dienstverlening en de op basis daarvan vastgestelde risico's. De risicoanalyse vormt de basis voor de inrichting van passende beheersmaatregelen, zoals het opstellen van prestatie-indicatoren (KPI's) en het vormgeven van continuïteit- en exit plannen. Dit wordt uiteindelijk vastgelegd in een overeenkomst.

1 Het uitbesteden van werkzaamheden die specifiek zien op het verrichten van beleggingsactiviteiten is niet meegenomen in dit onderzoek.

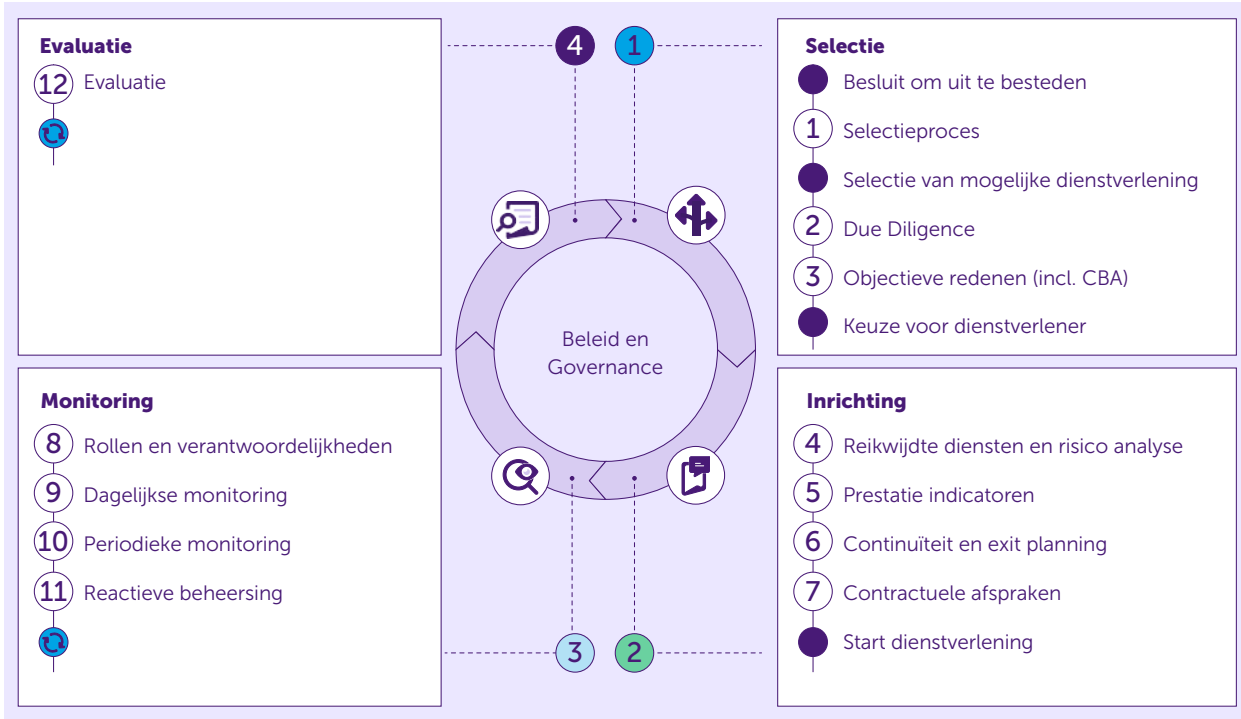
Fase 3. De monitoring van de uitbesteding.
De monitoring kan worden opgedeeld in doorlopende, periodieke en reactieve (event-driven) beheersing van de uitbestedingsrelatie. Per uitbestedingsrelatie zal verschillen op welke vorm van monitoring en welke monitoringsmaatregelen de nadruk ligt.

Fase 4. De evaluatie van de uitbestedingsrelatie.
In deze fase wordt periodiek beoordeeld of de relatie voortgezet moet worden.

De beheersing van de risico's van uitbesteding vindt vooral plaats gedurende de monitoring van bestaande uitbestedingsrelaties, maar begint al eerder in het proces. Essentieel voor de beheersing is het kwalificeren van de uitbesteding en de inrichting van de uitbestedings-relatie, waaronder het maken van afspraken met de dienstverlener en het vaststellen van welke beheersmaatregelen nodig zijn.

Naast de monitoringsfase (fase 3 in onderstaand figuur) zal de AFM in dit rapport dus ook stilstaan bij de inrichting van de uitbestedingen (fase 2 in onderstaand figuur) en de kwalificatie (onderdeel van het centrale deel in onderstaand figuur).

Figuur 1. De uitbestedingscyclus - In onderstaande uitbestedingscyclus zijn de vier fases afgebeeld, te weten selectie, inrichting, monitoring en evaluatie. Elke fase kent zijn eigen activiteiten.



1.3 Opzet van het onderzoek

De AFM wilde met dit onderzoek een beeld vormen van de mate waarin ondernemingen voldoende doen om de risico's van uitbesteding doorlopend te beheersen, en zo nodig handvatten te bieden voor die beheersing.

Het onderzoek kende twee fases. Eerst heeft de AFM een selectie gemaakt van 50 ondernemingen, variërend in omvang en activiteiten. Deze ondernemingen hebben een vragenlijst gekregen. Deze lijst bevatte vragen over bijvoorbeeld de recente omvang van de uitbesteding, de inrichting van de monitoring, welke functies betrokken zijn bij de monitoring en de risico's die ondernemingen zien.

Aan de hand van de uitkomsten van de vragenlijst is een selectie gemaakt van zes ondernemingen uit de eerdere selectie van 50 ondernemingen. Bij deze zes ondernemingen heeft een verdiepend gesprek over de monitoring van de uitbestedingen plaatsgevonden. Hier is gekeken hoe zij de doorlopende beheersing van uitbesteding praktisch vormgeven. Ook is met een aantal dienstverleners gesproken, om een beeld te krijgen van hun rol bij en visie op de beheersing van uitbesteding door en daaraan verbonden risico's bij ondernemingen.

1.4 Juridisch kader

Bij uitbesteding van werkzaamheden dienen ondernemingen zich te houden aan Nederlandse en Europese wet- en regelgeving. Deze regels zien ook op de monitoring van uitbesteding.

De AFM heeft eerder een schematisch overzicht van de relevante wettelijke vereisten per type onderneming gemaakt, opgenomen in tabel 1 van de Keten in Beeld sectorbrief van 28 november 2019. Deze is als bijlage 3 van dit rapport opgenomen. Verder zijn in zowel de sectorbrief uit 2019 als een Keten in Beeld sectorbrief uit 2021 diverse handvatten opgenomen voor de kwalificatie van de uitbesteding van werkzaamheden en de inrichting van beheersmaatregelen, waaronder monitoring.

Wanneer een onderneming twijfelt hoe beheersmaatregelen het beste kunnen worden ingericht volgens de regeling die op haar van toepassing is, kunnen handvatten over het beheersen van uitbestedingsrisico's uit hoofde van andere regelingen of van andere (toezichthoudende) organen, zoals de good practices van De Nederlandsche Bank of de richtsnoeren van De Europese Bankautoriteit (EBA)[2], mogelijk praktische diepgang bieden.

Het rapport gaat uit van de wet- en regelgeving zoals die op het moment van publicatie geldt. Na publicatie van dit rapport, op 17 januari 2025, zal DORA van kracht worden. Onderdeel hiervan zijn regels over het beheersen van ICT-diensten, waardoor er een samenhang is met dit rapport.

In dit rapport zijn aanbevelingen opgenomen voor de praktische invulling van de bestaande normen voor uitbesteding in het algemeen. Deze zijn in beginsel relevant voor alle uitbestedingen, ook voor ICT-uitbestedingen. Voor zover het opvolgen van bepaalde aanbevelingen in dit rapport onverenigbaar zou zijn met het naleven van de verplichtingen ingevolge DORA, dienen deze laatste met voorrang nageleefd te worden.

Voor zover er concrete aanbevelingen nodig zijn ten aanzien van ICT-uitbestedingen zijn deze meer passend binnen het kader van DORA. Daarom bevat dit rapport geen specifieke aanbevelingen over uitbestedingen met ICT-componenten. Wel heeft de AFM een aantal observaties gedaan over ICT-uitbestedingen tijdens dit onderzoek. Deze zijn wel opgenomen in het rapport.

Uitbesteding blijft naar verwachting van de AFM een onderwerp dat hoog op de agenda staat bij internationale wetgevings-en toezichthoudende instanties. Zo bevat de recent gepubliceerde AIFMD-herziening (Richtlijn (EU) 2024/927) ook verschillende ontwikkelingen op het gebied van uitbesteding. De AFM beveelt ondernemingen aan de ontwikkelingen nauwgezet op te volgen en, indien nodig, tijdig opvolging te geven.

2 Bijvoorbeeld de richtsnoeren voor uitbesteding van de European Banking Authority (EBA/GL/2019/02, 25 februari 2019), welke op dit moment niet van toepassing zijn op ondernemingen in de asset management sector (behoudens op klasse 1 beleggingsondernemingen). De richtsnoeren worden in de toekomst herzien waarbij de reikwijdte mogelijk wordt aangepast.

2. Bevindingen

Op hoofdlijnen resulteert het onderzoek van de AFM in vijf overkoepelende bevindingen. De eerste drie bevindingen zijn generiek, de twee laatste bevindingen zien op specifieke situaties. Bij de vijf bevindingen stelt de AFM in het volgende hoofdstuk aanbevelingen vast.

Bevinding 1 - Kwalificatie
Ondernemingen hebben niet altijd een goed onderbouwde aanpak voor het bepalen van wat gezien moet worden als uitbesteding en welke uitbesteding kwalificeert als materieel.

Als onderdeel van het onderzoek is een lijst met uitbestedingsrelaties opgevraagd, zowel materieel[3] als niet materieel. Bij navraag bleek dat het begrip uitbesteding meer dan eens te beperkt was uitgelegd. Ook bleek dat de wijze waarop ondernemingen vaststellen welke uitbesteding materieel is, vaak beperkt en niet consistent was en dat de onderbouwing beperkt was. Hierbij viel op dat de handvatten ten aanzien van de kwalificatie van uitbestedingen, zoals opgenomen in de Keten in Beeld sectorbrief uit 2019, regelmatig niet was gevolgd. Een verkeerde kwalificatie kan ertoe leiden dat er onvoldoende beheersingsmaatregelen worden genomen.

Bevinding 2 - Inrichting
Bij de inrichting van uitbestedingen denken ondernemingen vaak nog te beperkt na over maatregelen en afspraken die voorsorteren op een passende monitoring.

De monitoringswerkzaamheden rondom uitbesteding vinden (onder andere) plaats op basis van door de dienstverlener aangeleverde documenten, zoals rapportages en certificeringen. Dit vereist dat in een eerder stadium de risico's in kaart zijn gebracht, en dat op grond daarvan goede afspraken zijn gemaakt over welke prestaties en documenten de dienstverlener zal leveren. Uit het onderzoek bleek dat de link tussen deze eerdere inrichtingsfase en de latere monitoringsfase niet in alle gevallen voldoende was gelegd. Dit kan ertoe leiden dat er in de monitoringsfase onduidelijkheid ontstaat over de verantwoordelijkheden en rechten tussen de onderneming en de dienstverlener, waardoor risico's door de onderneming onvoldoende geïdentificeerd en beheerst worden.

3 De term 'materieel' wordt in dit rapport gebruikt om uitbestedingen aan te duiden van werkzaamheden die vallen binnen de reikwijdte van de uitbestedingsregels in de Wft en Europese sectorale regelgeving. Onder materieel wordt in dit rapport verstaan uitbesteding als bedoeld in de definitie van uitbesteding in artikel 1:1 Wft, kritiek en belangrijk als bedoeld in artikel 16, vijfde lid, MiFID II (Markets in Financial Instruments Directive (EU) 2014/65) en artikel 31 MiFID II Gedelegeerde Verordening 2017/565 en de functies als bedoeld in artikel 20 AIFMD en bijlage I van AIFMD (Alternative Investment Fund Management Directive (EU) 2011/61) en de functies als bedoeld in artikel 13 UCITS Richtlijn en bijlage II van de UCITS richtlijn (Undertakings for Collective Investment in Transferable Securities Directive, 2009/65/ec).

Bevinding 3 - Monitoring
Ondernemingen gaan zeer verschillend om met de monitoring van uitbestedingen en maken niet altijd gebruik van de meest geschikte methodes om de risico's van uitbesteding te beheersen; een meer consistente en uitlegbare aanpak op grond van risico's is noodzakelijk.

Ondernemingen moeten zelf bepalen welke vorm en frequentie van monitoring noodzakelijk is, afhankelijk van de specifieke risico's die gepaard gaan met een uitbesteding. De verwachting is dat de monitoring van uitbesteding van vergelijkbare werkzaamheden, met vergelijkbare risico's, op een vergelijkbare wijze zal plaatsvinden. In het onderzoek viel op dat het uitbesteden van vergelijkbare werkzaamheden bij verschillende ondernemingen anders gemonitord werd, wat niet altijd te verklaren was door de specifieke risico's. Zo gaan ondernemingen bijvoorbeeld zeer verschillend om met het beoordelen van certificeringen van de dienstverlener. Ook de vorm en frequentie van reviewgesprekken met de dienstverlener verschillen per onderneming, zelfs bij afname van dezelfde diensten. Deze verschillen waren vaak niet goed uitlegbaar. Het is belangrijk dat ondernemingen voldoende kunnen onderbouwen waarom zij kiezen voor een bepaalde vorm en frequentie van monitoring.

Bevinding 4 - Intra-groep
Voor intra-groep uitbestedingen wordt vaak (te) veel geleund op informele maatregelen en afspraken.

Binnen groepen wordt regelmatig gebruik gemaakt van structuren waarbij er gebruik wordt gemaakt van groepsmiddelen, bijvoorbeeld via centrale dienstverlening vanuit de groep ('shared services'). Ondernemingen zien dit vanuit praktisch oogpunt vaak niet als uitbesteding, terwijl het dit volgens de wet- en regelgeving vaak wel is. Ook de monitoring vindt in de praktijk vaak informeel en/of (te) beperkt plaats. Bij het wegen van de risico's kan de grip op de dienst die is uitbesteed en de groepsdienstverlener worden meegenomen, maar dit betekent niet dat er geen monitoring hoeft te worden ingericht. Hoewel vaak wordt aangenomen dat belangen binnen de groep altijd gelijk zijn, is dit in de praktijk niet het geval. Ondernemingen kunnen dan ook niet volledig steunen op de groepsfunctie en dienen zelf passende beheersmaatregelen te treffen.

Bevinding 5 - ICT specifiek
Ondernemingen zijn zich niet altijd bewust van ICT-componenten in uitbestedingen en de bijbehorende ICT-risico's.

Voor veel uitbestedingen maakt de dienstverlener gebruik van ICT, onder andere (web)applicaties, gegevensverwerking en -opslag. Deze ICT-componenten in een uitbesteding kennen echter eigen ICT-risico's. Ondernemingen staan niet altijd voldoende stil bij deze ICT-componenten en hun risico's, zoals risico's rondom de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte gegevens.

3. Aanbevelingen

In dit deel van het rapport geeft de AFM per bevinding, zoals beschreven in Hoofdstuk 2, een aantal aanbevelingen rondom de doorlopende beheersing van uitbestedingen. Ook bevat dit deel van het rapport specifieke observaties ten aanzien van ICT-uitbestedingen.

3.1 Kwalificatie

Ondernemingen hebben een verschillende aanpak ten aanzien van het bepalen van wat gezien moet worden als uitbesteding en welke uitbesteding kwalificeert als materieel. De AFM heeft hier eerder handvatten over gegeven in een sectorbrief inzake Keten in Beeld (zie bijlage IV bij dit rapport). Die handvatten gelden nog steeds maar lijken onvoldoende te zijn gevolgd.

De AFM geeft daarom een aantal aanbevelingen ten behoeve van een meer passende kwalificatie rondom uitbestedingen.

Aanbeveling 1 - Definitie
Stel schriftelijk beleid op waarin is uitgewerkt hoe op een eenduidige wijze wordt vastgesteld of sprake is van uitbesteding.

Het is belangrijk dat ondernemingen beleid en procedures opstellen waarin op een eenduidige manier vastgesteld wordt wanneer sprake is van uitbesteding. Hierbij kunnen ondernemingen de gezichtspunten betrekken die zijn genoemd in Bijlage II. Het is ook van belang om de analyses en de uitkomsten daarvan per situatie vast te leggen. Bij het doorlopen van de procedures moeten ook de onderuitbestedingen worden meegenomen. Van onderuitbesteding is sprake als de dienstverlener aan wie is uitbesteed, de betreffende werkzaamheden zelf ook (deels) uitbesteedt. Een onderneming die uitbesteedt is namelijk verantwoordelijk voor alle risico's. En daar vallen ook de onderuitbestedingen onder. Onderuitbesteding komt in het bijzonder veel voor in geval van het gebruik van ICT-systemen, bijvoorbeeld door de hosting van ICT-systemen in de cloud.

Uit het onderzoek van de AFM bleek dat veel ondernemingen relaties met derde partijen vaak zonder vastgelegde analyse of onderbouwing niet als uitbesteding kwalificeren. Het gaat dan met name om uitbesteding aan partijen waar gebruik wordt gemaakt van personeel, diensten of systemen. Veel ondernemingen zien dit als '*inkoop*', '*insourcen*', '*standaarddiensten*' of '*support*'. We constateren dat er in die gevallen regelmatig wel degelijk sprake is van uitbesteding.

Door een verkeerde kwalificatie worden mogelijke risico's in die gevallen onvoldoende in kaart gebracht en zijn de beheersmaatregelen veelal onvoldoende. Zo namen ondernemingen regelmatig aan dat de uitzondering in MiFID II ten aanzien van standaarddiensten breed konden worden toegepast, zoals voor software. Het begrip standaarddienst dient nauw te worden geïnterpreteerd, zo vallen niet alle 'off-the-shelf' producten hier per definitie onder.

Aanbeveling 2 - Materieel
Leg in de schriftelijke procedures vast hoe wordt vastgesteld welke werkzaamheden gezien worden als materieel. Hanteer daarbij een niet te nauwe interpretatie van deze begrippen.

Het is van belang om in het schriftelijk beleid en procedures op een eenduidige manier te beschrijven hoe wordt vastgesteld of er sprake is van materiële werkzaamheden. Net als bij de kwalificatie van uitbesteding, is het ook hier van belang dit per uitbestedingsrelatie vast te leggen.

Voor de volledigheid merken we op dat ondernemingen altijd passende beheersmaatregelen dienen te treffen om een beheerste bedrijfs-

voering te waarborgen. Dat betekent dat zelfs als werkzaamheden niet materieel zijn, er wel passende beheersmaatregelen dienen te worden genomen.

De term 'materieel' wordt in dit rapport gebruikt om uitbestedingen aan te duiden van werkzaamheden die vallen binnen de reikwijdte van de uitbestedingsregels in de Wft en Europese sectorale regelgeving en waar dus geen uitzondering op van toepassing is. Onderstaand is dit verder toegelicht voor ondernemingen die onder MiFID II vallen en ondernemingen die onder AIFMD vallen.

Ondernemingen die onder MiFID II vallen bleken regelmatig ten onrechte aan te nemen dat diensten niet materieel zijn. De uitleg was dan bijvoorbeeld dat er alternatieven beschikbaar waren of dat de diensten niet zien op een uitbesteding van een primair proces. Het criterium 'kritiek en belangrijk' dat geldt op grond van het MiFID II kader dient echter breed uitgelegd te worden. Zo is het niet alleen belangrijk of de continuïteit van de onderneming in gevaar komt wanneer zich problemen voordoen in de uitbestedingsrelatie, maar ook of de onderneming door problemen van de uitbestede dienst niet langer aan de verplichtingen van de wet- en regelgeving kan voldoen. Hierdoor zullen in de praktijk veel uitbestedingsrelaties wel als kritiek of belangrijk moeten worden aangemerkt. Zo zijn ook diensten als financiële administratie en ondersteuning van de controlefuncties (compliance, risicomanagement en internal audit) in beginsel uitbesteding van 'kritieke of belangrijke' functies of werkzaamheden ondersteunend daaraan.

Ondernemingen die onder AIFMD vallen leken regelmatig een te nauwe reikwijdte te hanteren van de uitbestedingsregels in de AIFMD, mede op basis van een te restrictieve interpretatie van de diensten die zijn genoemd in Bijlage I AIFMD. De begrenzing van de uitbestedingsregels onder AIFMD ziet op ondersteunende taken en deze dienen beperkt te worden uitgelegd (denk aan catering, schoonmaak, en 'one-off' expertise en advisering).

Het kwam in het kader van vastgoedbeheer voor dat andere werkzaamheden dan het dagelijkse operationele beheer op objectniveau niet werden gezien als onderdeel van Bijlage I AIFMD, terwijl dit wel het geval is. Zie hiervoor ook punt 2 (c) van Bijlage I AIFMD, verwijzing naar faciliteitenbeheer en vastgoedbeheer. In beginsel blijft dit ook zo onder de AIFMD-herziening.

3.2 Inrichting

De inrichting van de uitbestedingsrelatie is essentieel voor een goede monitoring. Bij de inrichting van uitbestedingen denken ondernemingen niet altijd voldoende na over maatregelen en afspraken die voorsorteren op een passende doorlopende beheersing. Hieronder geeft de AFM een aantal aanbevelingen ten behoeve van een meer passende inrichting van uitbestedingsrelaties.

Aanbeveling 3 - Beleid en procedures
Stel schriftelijke procedures op waarin **per uitbestedingsrelatie** wordt uitgewerkt hoe uitbestedingsrisico's geïdentificeerd en beheerst worden.

Schriftelijk beleid en procedures zijn fundamenteel voor de continue beheersing van mogelijke risico's rondom uitbestedingsrelaties. Uit het onderzoek bleek echter dat de schriftelijke procedures vaak te veel op hoofdlijnen waren opgesteld, waardoor er geen gestructureerd proces met betrekking tot monitoring was vastgelegd.

Uit een procedure zou moeten volgen hoe, wie, wat, wanneer doet ten behoeve van de doorlopende beheersing van uitbestedingsrisico's. Het is daarom goed om een procedure per uitbestedingsrelatie op te stellen waarin dit wordt uitgewerkt. Voor een eenduidige en efficiënte aanpak zijn ondernemingen tevens gebaat bij het opstellen van standaard sjablonen en templates, bijvoorbeeld met vaste review criteria of evaluatiepunten.

Aanbeveling 4 - Integraal overzicht
Houd een integraal overzicht bij, met daarin een aantal essentiële elementen van alle uitbestedingsrelaties die zijn aangegaan.

Uit het onderzoek bleek dat ondernemingen niet in alle gevallen een overzicht hadden van uitbestedingsrelaties. Hierdoor was het proces om te achterhalen welke uitbestedingen er daadwerkelijk waren soms ingewikkeld en langdurig. Om uitbestedingen en daarmee gepaarde risico's te beheersen, is het hebben van een integraal overzicht essentieel. Dit overzicht zou in ieder geval de volgende belangrijke elementen van uitbestedingsrelaties moeten bevatten[4]:

1. een uniek nummer voor elke uitbestedingsrelatie;
2. belangrijke informatie over de dienstverlener, zoals naam, adres en contactgegevens;
3. de startdatum, datum van contractverlenging, en/of de einddatum van de uitbestedingsovereenkomst, inclusief eventuele opzegtermijnen;
4. het type dienst dat is uitbesteed;
5. de kwalificatie van de dienst als materieel of niet materieel;
6. of er sprake is van een ICT dienst, incl. het type data dat gepaard gaat met de uitbesteding;
7. het land waarvandaan de dienst wordt uitgevoerd/waar de data verwerkt wordt;
8. essentiële informatie over onderuitbestedingen.

Dit is geen limitatieve lijst. Iedere onderneming dient zelf te beoordelen welke informatie nuttig is om bij te houden in dit overzicht.

Aanbeveling 5 - Risicoanalyse
Voer zowel ex-ante als ten minste jaarlijks een risicoanalyse uit. Stel daarna voor iedere uitbesteding vast welke beheersmaatregelen passen bij de uitbesteding.

Het is belangrijk dat ondernemingen voorafgaand aan het aangaan van een uitbestedingsrelatie een risicoanalyse uitvoeren. Het doel is om vast te stellen welke beheersmaatregelen moeten worden genomen. Bij een risicoanalyse kan onder meer gekeken worden naar de aard en het type prestatie-indicatoren, het gebruik van toegangsrechten, informatie- en auditrechten, de frequentie en inhoud van rapportages, certificering, review- en escalatiemogelijkheden.

Een risicoanalyse dient tenminste jaarlijks herhaald te worden om eventuele wijzigingen in risico's te identificeren en beheersmaatregelen desgewenst tijdig aan te passen. In geval van bijzonderheden, zoals wijzigingen of incidenten, kan het nodig zijn de risicoanalyse op ad-hoc basis te evalueren en waar nodig te herzien.

De risicoanalyse wordt in beginsel uitgevoerd door de eerstelijnsfuncties, met controle en betrokkenheid van de tweedelijns riskfunctie. Deze functies moeten dus over voldoende kennis beschikken van mogelijke risico's die gepaard gaan met uitbesteding en de werkzaamheden die worden uitbesteed.

Het ligt voor de hand dat de maatregelen niet bij alle uitbesteding hetzelfde zullen zijn omdat de risico's van de uitbesteding kunnen verschillen. Zo zullen de risico's van uitbesteding van compliance en risk-functies vaak met name zien op kwaliteit en tijdigheid, waarbij beheersing door middel van regelmatige reviewgesprekken een van de passende middelen kan zijn. Bij uitbesteding van vermogensbeheer kunnen de risico's eenvoudiger kwantitatief worden gemeten, waardoor als beheersingsmaatregelen (mede) gebruik kan worden gemaakt van rapportages, certificeringen en informatie- en auditrechten.

4 Dit zijn enkele van de vereisten die met de inwerkingtreding van DORA gelden met betrekking tot een register als er sprake is van overeenkomsten over het gebruik van door derde aanbieders verleende ICT-diensten, zie art. 28, derde lid, DORA. Ook de ESMA richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten bevat regels over een register voor clouddiensten. Deze vereisten zouden ook voor andere vormen van uitbesteding kunnen worden gebruikt.

Aanbeveling 6 - Verantwoordelijkheid
Beleg de (eind)verantwoordelijkheid voor de uitbestedingsrelatie en de monitoringsactiviteiten bij specifieke personen, die beschikken over passende kennis en ervaring. Zorg voor een duidelijke taakverdeling binnen het bestuur, met aandacht voor onder wie welke uitbesteding valt.

Het bleek dat de meeste ondernemingen voor alle uitbestedingen een specifieke bestuurder aanstellen als eindverantwoordelijke. Het gaat dan meestal om de bestuurder die het betreffende proces al in de portefeuille heeft. De eindverantwoordelijkheid voor de uitbesteding van de compliance en risk functie of taken worden vaak belegd bij de Chief Compliance Officer of Chief Risk Officer. Eerstelijnsfuncties worden vaak belegd bij de Chief Operational Officer of Chief Investment Officer. De verantwoordelijkheid voor de interne auditfunctie ligt over het algemeen bij de Chief Executive Officer.
Een aantal ondervraagde ondernemingen koos ervoor om niet een of meerdere specifieke verantwoordelijke bestuurders aan te stellen. Hiervoor werden de volgende redenen gegeven:

1. De verantwoordelijkheid voor de uitbestedingsrelatie wordt collectief gedragen.
2. De verantwoordelijkheid is niet toegewezen aan het bestuur, maar bijvoorbeeld wel op lager (management)niveau.
3. De verantwoordelijkheid ligt buiten de onderneming, bijvoorbeeld bij een groepsentiteit of bij de derde partij aan wie is uitbesteed.

Dit leidt volgens de AFM niet tot een goede governance van de uitbesteding. Het bestuur als collectief is eindverantwoordelijk voor de onderneming, inclusief uitbestedingen. Omdat niet iedereen in het bestuur hetzelfde doet, is het goed een taakverdeling af te spreken en vast te leggen. Houd in die taakverdeling rekening met de kennis en ervaring van de bestuurder van de uitbestede taak. Het niet aanwijzen van een specifieke verantwoordelijke bestuurder verkleint de kans dat op bestuursniveau voldoende verantwoordelijkheid kan worden genomen voor de uitbestede werkzaamheden.

Daarnaast zijn er meer medewerkers betrokken bij de monitoring van uitbesteding, zoals de eerstelijns monitoring en de risk en/of compliance functie. Naast dat hun verantwoordelijkheden duidelijk moeten zijn, moeten zij ook de juiste kennis en ervaring er voor hebben.

Aanbeveling 7 - Contractuele afspraken
Maak contractuele afspraken waarin is vastgelegd op welke wijze de dienstverlening wordt gemeten, wie daarvoor verantwoordelijk is, welke onderwerpen minimaal in de rapportage worden opgenomen en wat de rapportagefrequentie is.

Ondernemingen moeten goede contractuele afspraken te maken over de dienstverlening en wat de onderneming nodig heeft voor de monitoring. Deze afspraken worden vastgelegd in een overeenkomst. Hier gelden een aantal wettelijke vereisten voor. Zo dient de overeenkomst, waarmee we ook een service level agreement (SLA) bedoelen, in elk geval een heldere beschrijving van de dienstverlening te omvatten en moeten inspectie- en auditrechten worden vastgelegd. Daarnaast moeten in de overeenkomst ook de belangrijkste zaken voor de monitoring worden vastgelegd, zoals:

1. De prestatiedoelen;
2. De inhoud en frequentie van rapportages;
3. De informatie die dienstverlener over zijn beheersmaatregelen geeft aan de onderneming, bijvoorbeeld het soort en de frequentie van certificeringen en externe audits;
4. De procedure bij incidenten van de dienstverlener en het oplossen van de incidenten;
5. Het proces rondom het gebruik van onderuitbesteding, inclusief de nodige informatie-uitwisseling die nodig is voor het beheersen van de risico's van de onderuitbesteding;
6. De escalatielijn bij mogelijke problemen in de dienstverlening. De voorkeur geniet dat bij de mitigatie van het probleem niet alleen gekeken wordt naar senioriteit, maar ook naar wie de kennis of vaardigheden in huis heeft. Zo nodig wordt een werknemer op lager niveau betrokken;

7. De wijze waarop de onderneming door de dienstverlener geïnformeerd wordt bij impactvolle wijzigingen (o.a. onderuitbesteding) die de uitbestede dienst raken;
8. Afspraken rondom een (veelal) jaarlijkse review van de uitbesteding, en ad-hoc gesprekken als daar aanleiding voor is;
9. Het testen van het business continuïteitsplan van en door de dienstverlener, inclusief de rapportage hierover, aan de onderneming.

Aanbeveling 8 - Afspraken escalatie
Richt een escalatiestructuur in met escalatiemogelijkheden op verschillende niveaus en, indien relevant, voor zowel operationele functies, als tweedelijnsfuncties.

Het vooraf opstellen van een escalatiestructuur is van belang om, wanneer nodig, tijdig te kunnen reageren op problemen of zorgen. De escalatiestructuur bevat escalatiemogelijkheden op verschillende niveaus bij de onderneming. Zo kan een beperkt operationeel probleem dat spoed vereist direct worden geëscaleerd op werkvloer niveau en in gesprek met de dienstverlener. Daarnaast kan een significant probleem ook geëscaleerd worden naar de relevante eindverantwoordelijke in het bestuur.

In de escalatiestructuur wordt, indien relevant, ook nagedacht over verschillende escalatiemogelijkheden voor de operationele functies, en voor de tweedelijnsfuncties. Bij meer operationele risico's zal de eerste lijn primair betrokken worden. De tweede lijn moet betrokken worden als bepaalde risico's zich voordoen, denk bijvoorbeeld aan privacy gerelateerde risico's.

3.3 Monitoring

Onder monitoring van uitbesteding vallen zowel de doorlopende, de periodieke als ook de reactieve (event-driven) beheersing van de uitbestedingsrelatie. Onder doorlopende prestatiemonitoring wordt vooral verstaan het dagelijkse monitoren door de eerste lijn en de gebruikelijke hulpmiddelen daarbij, zoals dashboards en rapportages. Bij de periodieke monitoring wordt op een vast moment de dienstverlening getoetst en hebben ook de controlefuncties vaak een belangrijke rol. Hierbij kunnen ondernemingen gebruikmaken van het recht op informatie, inspectie en toegang, zoals een auditrapportage. Monitoring vindt niet alleen dagelijks en periodiek plaats, maar daarnaast kunnen ook activiteiten nodig zijn door bepaalde gebeurtenissen of afwijkingen. Denk hierbij vooral aan incidenten bij de onderneming en/of de dienstverlener en wijzigingen in de dienstverlening.

De AFM ziet dat ondernemingen zeer verschillend omgaan met de monitoring en niet altijd de risico's van de uitbesteding goed beheersen. Hieronder geven we aanbevelingen ten behoeve van een passende monitoring van uitbesteding.

Aanbeveling 9 - 3 Lines of Defence (3 LoD)
Wijs ook in geval van uitbesteding taken en verantwoordelijkheden toe aan operationele functies ('eerste lijn') en controlefuncties ('tweede en derde lijn') voor het monitoren van de uitbestedingsrelatie (3 LoD).

Binnen een onderneming is de eerste lijn primair verantwoordelijk voor de monitoring van de uitbestede taken. Dit gebeurt door het analyseren en controleren van de prestaties van de dienstverlener op dagelijkse basis. De aanwezigheid van personeel dat voldoende kennis, capaciteit en middelen heeft om deze taken te vervullen is vereist.

Het is vervolgens de verantwoordelijkheid van de tweedelijnsfuncties (risk en compliance) om periodiek te controleren dat de monitoring adequaat is ingericht en uitgevoerd. De derde lijn, of de auditfunctie, wordt betrokken bij het periodiek toetsen van het proces rondom de uitbestedingsrelatie en de monitoring daarvan.

Voor de uitbesteding van controlefuncties is de eerste lijn in beginsel niet betrokken bij de monitoring van de uitbestedingsrelatie en ligt de verantwoordelijkheid direct bij de tweede en derde lijn. Als de

controlefunctie uit één persoon bestaat en de functie is uitbesteed, ligt de verantwoordelijkheid voor monitoring bij een van de bestuurders.

Als er sprake is van een uitbesteding van eerstelijnsfuncties is het niet wenselijk dat er enkel taken en verantwoordelijkheden worden gealloceerd aan de controlefuncties voor het monitoren van de uitbestedingsrelatie.

Aanbeveling 10 - Control Framework
Houd een centraal control framework bij waarin de beheersmaatregelen worden vastgelegd.

Een goed gedocumenteerd centraal control framework is belangrijk omdat hier is vastgelegd hoe in alle gevallen consistent en afgewogen de risico's gemitigeerd worden. Het control framework bevat per uitbestedingsrelatie en per beheersmaatregel informatie over de actie die ondernomen moet worden om de beheersmaatregel uit te voeren, wie verantwoordelijk is binnen de organisatie, met welke frequentie en wat de uiterste datum van het uitvoeren van de controle is, welke rapportage en vastlegging gedaan moet worden en wat de status is van de (werking van de) beheersmaatregel.

Het control framework is niet statisch. De beheersmaatregelen zijn gekoppeld aan een risicoanalyse, omdat deze tot doel hebben om risico's te mitigeren. Risicoanalyses moeten periodiek of na een incident worden herijkt. Hiermee dient zo nodig ook het control framework te worden aangepast.

Aanbeveling 11 - Prestatie-indicatoren (KPI's) rapportages
Monitor de uitbesteding door middel van zowel kwantitatieve als kwalitatieve KPI's en gebruik daarbij rapportages met een passende frequentie.

Zoals genoemd in aanbeveling 7 is het belangrijk om contractuele afspraken te maken over de prestatiedoelen. Met behulp van kwantitatieve en kwalitatieve prestatie-indicatoren kunnen de dienstenniveaus die zijn afgesproken doorlopend gemonitord worden zodat zo nodig direct corrigerende maatregelen kunnen worden getroffen. Adequate KPI's kunnen daarnaast bijdragen aan een effectieve aansturing van de dienstverlener.

Nadat de prestatiedoelen zijn vastgelegd is de volgende stap om deze doelen meetbaar te maken en om te zetten naar kwantitatieve en kwalitatieve prestatie-indicatoren. Kwantitatieve prestatie-indicatoren zijn bijvoorbeeld het aantal uren dat iemand een functie uitoefent of de benchmark bij vermogensbeheer. Kwalitatieve prestatie-indicatoren zien bijvoorbeeld op de tevredenheid over de dienstverlening of de kwaliteit van incidentafhandeling.

Vervolgens kunnen met de dienstverlener afspraken gemaakt worden over de frequentie en toegang tot rapportages over de afzonderlijke KPI's. Deze rapportages kunnen op verschillende manieren beschikbaar gesteld worden: schriftelijke rapportages via mail, toegang tot een dashboard, of toegang tot de systemen waaruit de benodigde rapportages opgevraagd kunnen worden. Tot slot is het belangrijk om in de rapportages niet alleen te kijken of de gemaakte afspraken over dienstniveaus worden nagekomen, maar ook te kijken naar de trends en ontwikkelingen die op langere termijn grenswaarden overschrijden. Bijvoorbeeld door het opstellen van een preventieve grenswaardes en proactieve *alerting*, zoals 10% toename van oplostijd voor incidenten of 1 minuut uitvaltijd van een portaal, kan voorkomen worden dat deze negatieve trend zich ongemerkt doorzet op de langere termijn en de KPI uiteindelijk niet gehaald wordt. De prestatiedoelen kunnen periodiek geëvalueerd worden samen met de dienstverlener.

De AFM vindt dat in beginsel zowel kwantitatieve criteria als kwalitatieve criteria moeten worden gebruikt om volledig inzicht te hebben in de prestaties. Hierbij is het van belang om het samenstel van kwantitatieve en kwalitatieve criteria af te stemmen op de specifieke uitbestedingsrelatie.

Aanbeveling 12 - Audit rapportages
Review beschikbare audit rapportages van derden periodiek op de geldigheid, scope, diepgang en bevindingen van deze rapporten.

Beschikbare audit rapportages moeten worden meegenomen in de periodieke monitoring. Zij geven een dieper inzicht in de interne beheersing van de uitbestede processen en of deze in overeenstemming is met gemaakte afspraken of geldende standaarden. Een audit kan door de onderneming uitgevoerd worden bij de dienstverlener of door een onafhankelijke partij in opdracht van de onderneming bijvoorbeeld als onderdeel van een certificering. Op basis van het audit-/informatierecht in een contract stellen veel dienstverleners zelf certificeringen of assurance rapportages beschikbaar, om het aantal audits van hun afnemers te verlagen. De onafhankelijkheid van deze rapportages kan geborgd worden door dit te laten uitvoeren door een externe partij op basis van internationaal erkende standaarden.

Een bekend voorbeeld zijn de jaarrekening controles of een ISAE3402 verklaring. In de ISAE3402 worden de controls van de dienstverlener getoetst, waaronder de financiële beheersmaatregelen en de ICT-beheersmaatregelen kunnen vallen. Om de beheersmaatregelen rondom informatiebeveiliging te toetsen zijn er een aantal specifiekere audit rapportages die vaak gehanteerd worden, zoals een ISO27001 certificering of een SOC2-type II (ISAE 3000) rapport. Rapportages geven via een onafhankelijke auditor inzicht in de controls die dienstverlener heeft opgezet en/of gebruikt en zijn internationaal erkend. De diverse rapportages zijn verschillend in methodiek en diepgang.

Voor de periodieke monitoring is het daarom voor een onderneming belangrijk om na te denken welke (onafhankelijke) audit rapportages nodig zijn om meer inzicht te krijgen in de beheersing van de uitbestede werkzaamheden door de dienstverlener. Beschikbare audit rapportages dienen vervolgens aangeleverd te worden om deze zelf te kunnen beoordelen. Besteed bij de evaluatie aandacht aan de geldigheid, scope en diepgang van de ontvangen rapportages. De onderneming bespreekt vervolgens hun evaluatie met de dienstverlener en bewaakt de oplossing van eventuele bevindingen. Als de beschikbare audit rapportages onvoldoende zijn om de interne beheersing voldoende te toetsen, dan dient de onderneming te overwegen zelf periodiek een audit uit te voeren of te laten uitvoeren.

Aanbeveling 13 - Incidenten bij de dienstverlener
Stel een helder en gedocumenteerd incidentenprocedure op met betrekking tot incidenten bij de dienstverlener.

Als zich een incident bij de dienstverlener voordoet zorgt een vooraf opgestelde procedure er voor dat eventuele negatieve gevolgen voor de onderneming beperkt worden. Het is daarom ook belangrijk om met de dienstverlener afspraken te maken over het oplossen van incidenten. Daarbij moet onder meer een heldere taakverdeling voor alle betrokken partijen worden vastgelegd en afspraken worden gemaakt over communicatie bij impactvolle incidenten. Het is van belang dat ondernemingen toegang hebben tot informatie met betrekking tot incidenten. Voortgang kan bewaakt worden, bijvoorbeeld door toegang tot het ticketingsysteem van de dienstverlener. Hiermee kunnen ondernemingen het incidentenbeheer effectief monitoren.

Een incident bij een dienstverlener kan een gevaar vormen voor de integere bedrijfsvoering van de onderneming en daarmee vallen onder de wettelijke verplichting van een onderneming om incidenten onverwijld te melden bij de AFM. Een voorwaarde om aan deze meldingsplicht te kunnen voldoen, is het maken van afspraken met de dienstverlener over het opleveren van incidentrapportages, met een root cause analyse en een actieplan.

3.4 Intra-groep uitbesteding

Voor intra-groep uitbestedingen wordt doorgaans (te) veel geleund op informele maatregelen en mindere zwaar ingevulde maatregelen. Daarbij gaan ondernemingen er van uit dat het groepsbelang altijd gelijkloopt aan het ondernemingsbelang en de verschillende klantbelangen. Dit is niet in alle situaties het geval.

Daarom moet in beginsel alles dat voor externe uitbestedingen ingeregeld wordt, ook ingeregeld worden voor intra-groep uitbestedingen. Hier is de wet, en de toelichting daarop, helder over. Bovenstaande aanbevelingen zijn dus ook bedoeld voor intra-groep uitbestedingen. Op onderdelen kan het wel passend zijn om voor intra-groep uitbestedingen andere nuances aan te brengen. Hieronder geeft de AFM een aantal aanbevelingen en verduidelijkingen, specifiek ten behoeve van intra-groep uitbestedingen.

Aanbeveling 14 - Personele ondersteuning vanuit de groep
Neem bij intra-groep uitbesteding in het schriftelijke beleid mee dat personele ondersteuning vanuit groepsentiteiten vaak als uitbesteding kwalificeert. Gebruik daarnaast de juiste beheersmaatregelen.

Ondernemingen kwalificeren vaak personele ondersteuning vanuit de groep (vaak genoemd 'shared services' of 'support') ten onrechte niet als uitbesteding. Deze ondersteuning is niet bij voorbaat uitgezonderd van de uitbestedingsregels. Ook zijn er vaak dezelfde risico's aanwezig, waardoor beheersmaatregelen nodig blijven. Wel kan het zijn dat er invloed kan worden uitgeoefend door de onderneming op de maatregelen die de dienstverlener treft. Hier kan dan wel rekening mee gehouden worden, bijvoorbeeld bij de diepgang van sommige beheersmaatregelen.

Daarnaast zien we bij ondernemingen personele ondersteuning vanuit de groep wel als uitbesteding aanmerken regelmatig dat ze onvoldoende beheersmaatregelen treffen omdat ze dit niet nodig vinden gezien de groepssituatie.

De kwalificatie kan inderdaad complex zijn. Het schema in Bijlage II bevat daarom gezichtspunten die kunnen worden gebruikt om in kaart te brengen of er al dan niet sprake is van uitbesteding.

Aanbeveling 15 - Beheersing van risico's van intra-groep
Zorg ook bij intra-groep uitbestedingen voor passende beheersmaatregelen, die aansluiten bij de intra-groep praktijken en risico's die daaruit voortvloeien.

Een onderneming blijft ook bij intra-groep uitbesteding zelf verantwoordelijk voor de beheersing van mogelijke risico's van uitbesteding. Het enkele feit dat er sprake is van een intra-groep uitbesteding, is dan ook op zichzelf geen reden om gebruik te maken van beperktere beheersingsmaatregelen.

Bij intra-groep uitbestedingen kan (gedeeltelijk) gebruik worden gemaakt van groepsbeleid en procedures, om zo een eenduidig beleid te voeren binnen de groep. Dit vereist dan wel in elk geval eigen gedocumenteerde procedures waarin staat beschreven hoe de onderneming deze beheersing realiseert. Hierbij kan rekening worden gehouden met de belangen van de onderneming ten opzichte van de groep of de invloed van de onderneming op de dienstverlener.

Een beroep op het proportionaliteitsbeginsel is ook niet vanzelfsprekend voor intra-groep uitbestedingen. Ook een beroep op artikel 31 lid 4 van de MiFID gedelegeerde verordening 2017/565 – op grond waarvan rekening gehouden mag worden met de mate waarin de onderneming zeggenschap heeft over de dienstverlener of invloed kan uitoefenen op diens handelingen bij het voldoen aan de uitbestedingsverplichtingen – is niet gerechtvaardigd voor elke intra-groep uitbesteding. Er kan niet zomaar aangenomen kan worden dat men binnen de groep daadwerkelijk de mogelijkheid heeft invloed uit kunnen oefenen op de handelingen van de dienstverlener. Zeker niet wanneer de dienstverlener de moedermaatschappij betreft.

Daarbij kunnen ondernemingen er niet per definitie vanuit gaan dat er sprake is van minder risico's bij intra-groep uitbestedingen. Wel is het zo dat intra-groep uitbestedingen vaak een ander risicoprofiel kennen en dit kan meegenomen worden in de inrichting van de uitbestedingsrelatie en de bijbehorende beheersmaatregelen. Denk hierbij bijvoorbeeld aan directe toegang tot systemen of personen, die invloed kunnen hebben op het type, de frequentie, of de intensiteit van benodigde rapportages.

Bij intra-groep uitbesteding kan er ook een passende invulling worden gegeven aan de wettelijke eisen rondom uitbestedingen. Zo kan de kosten-batenanalyse bijvoorbeeld in sommige gevallen beknopter zijn, waarbij het kostenkader van meerdere externe dienstverleners minder uitgebreid in kaart kan worden gebracht. Het is echter wel van belang dat de kosten voor de dienstverlening ook bij uitbestedingen binnen de groep worden vastgesteld, mede om een heldere kostenvergelijking en afweging te kunnen maken bij de (doorlopende) aanstelling van een dienstverlener.

Aanbeveling 16 - Afspraken intra-groep
Leg ook bij intra-groep uitbestedingen de afspraken met betrekking tot de monitoring van intra-groep uitbesteding vast in een contract.

Het opstellen van een schriftelijke uitbestedingsovereenkomst is, ook voor intra-groep uitbestedingen, een wettelijk vereiste. De AFM constateert dat ondernemingen hier over het algemeen voldoen, maar dat de overeenkomsten met name bij intra-groep uitbestedingen onvoldoende specifiek zijn.

Als er binnen de groep wordt uitbesteed worden er specifieke contractuele afspraken gemaakt, waarin voldoende duidelijk wordt vastgelegd dat de onderneming zelf verantwoordelijk blijft voor de uitbestede werkzaamheden. Ten aanzien van monitoring is het ook in het geval van intra-groep uitbesteding van belang dat de reikwijdte van de diensten en werkzaamheden duidelijk wordt gespecificeerd, er duidelijke kwalitatieve en kwantitatieve prestatie indicatoren worden overeengekomen en er contractuele afspraken worden gemaakt rondom rapportage en evaluatie van de uitbestede diensten. Dit geldt voor alle type intra-groep uitbestedingen.

Aanbeveling 17 - Intra-groep belangen
Maak een schriftelijke analyse specifiek ten aanzien van intra-groep belangenconflicten en leg deze vast.

Uit het AFM-onderzoek bleek dat het identificeren, voorkomen en beheersen van mogelijke belangenconflicten niet altijd nadrukkelijk aandacht krijgt bij intra-groep uitbestedingen. Vaak wordt ervan uitgegaan dat alle belangen binnen de groep gelijklopen.

De AFM constateert dat er, in elk geval op onderdelen van de relatie, wel degelijk belangen kunnen zijn die uiteen kunnen lopen. Een voorbeeld is het alloceren van middelen over de entiteiten heen. Het doen van een gedegen analyse op dit gebied, zowel bij het initiëren van de uitbestedingsrelatie, als op doorlopende basis, is daarom van belang.

Aanbeveling 18 - Duale functies (dubbele petten)
Stel een gedocumenteerd proces op rondom duale functies (dubbele petten) en daarmee samenhangende potentiële belangenconflicten.

Uit het onderzoek van de AFM bleek dat ingeval van intra-groep uitbestedingen er vaak sprake is van 'dubbele petten' waarbij dagelijks beleidsbepalers, managers en werknemers zowel een rol hebben bij de onderneming, als bij de intra-groep dienstverlener. Het is in dan niet altijd duidelijk in welke hoedanigheid of vanuit welke rol de betrokken werknemer werkzaamheden uitvoert.

Het is daarom belangrijk een (lokale) eindverantwoordelijke aan te stellen in het bestuur als binnen de groep wordt uitbesteed. Een

dubbele pet kan in dit geval alleen als er naast de eindverantwoordelijkheid over de uitbestedingsrelatie geen directe betrokkenheid is bij de uitbesteding vanuit de interne dienstverlener.

Verder is het in die gevallen extra belangrijk dat is vastgelegd hoe bij dergelijke dubbele functies in geval van uitbesteding de rollen en verantwoordelijkheden zijn verdeeld en hoe wordt omgegaan met potentiële belangenconflicten.

Aanbeveling 19 - Groepsmonitoring
Leg de eigen verantwoordelijkheden van de monitoringsactiviteiten vast als een groepsentiteit tevens (gedeeltelijk) de monitoring van de (intra-groep) uitbesteding uitvoert.

Als er binnen een groep werkzaamheden worden uitbesteed, moet er ook monitoring plaatsvinden. Soms wordt dan ook een deel van de monitoringsactiviteiten door personen binnen de groep uitgevoerd. Het is in die gevallen goed om de taken en verantwoordelijkheden tussen de onderneming en de (groeps)dienstverlener vooraf duidelijk te definiëren en documenteren. Hierbij dient ook rekening te worden gehouden met mogelijke belangenconflicten. Het is daarbij van belang te borgen dat de beheersing van de uitbestedingsrisico's nog voldoende autonoom en onafhankelijk kan plaatsvinden.

Als er binnen de groep wordt uitbesteed en ook de monitoring van de uitbesteding door een groepsentiteit wordt uitgevoerd, dan blijft de onderneming verantwoordelijk en controleert zij tevens dat de monitoring adequaat wordt uitgevoerd. Dit vereist in elk geval een check van de monitoring zoals aan de hand van monitoringsrapportages. De onderneming legt de controles in een verslag vast.

In geval van uitbesteding van werkzaamheden naar een groepsentiteit, kan er sprake zijn van onderuitbesteding als er binnen de groep centraal contracten met dienstverleners worden gesloten. De regels over onderuitbesteding zijn dan ook onverkort van toepassing.

Aanbeveling 20 - Escalatie bij intra-groep uitbesteding
Zorg er voor dat er tot op niveau van het bestuur van de onderneming kan worden geëscaleerd.

Als er binnen de groep wordt uitbesteed moet het personeel van de onderneming de mogelijkheid hebben om problemen bij de intra-groep dienstverlener tot op het niveau van het bestuur van de onderneming te escaleren.

We hebben gezien dat in sommige gevallen er geen escalatie naar het bestuur van de onderneming was, maar naar een groepsentiteit. Daarom wijzen we erop dat de escalatie mogelijkheden niet alleen naar een groepsentiteit moeten worden ingeregeld, om mogelijke belangenconflicten binnen de groep te voorkomen.

3.5 Gebruik van ICT van derde partijen

De bedrijfsvoering van financiële ondernemingen is in toenemende mate afhankelijk geworden van ICT-middelen. Hierdoor zijn de ICT-risico's ook toegenomen. Deze ontwikkeling heeft ook gevolgen voor situaties waarin de financiële onderneming gebruik maakt van ICT die wordt geleverd door derde partijen.

De AFM doet in dit rapport geen aanbevelingen ten aanzien van het beheersen van ICT-risico's bij uitbesteding. De reden hiervoor is dat ondernemingen vanaf 17 januari 2025 zullen moeten voldoen aan de vereisten uit DORA. DORA bevat gedetailleerde vereisten op het gebied van het gebruik van ICT-diensten van derde partijen. Naar verwachting zullen de Europese toezichthoudende autoriteiten nog met aanvullingen en guidance (zoals Q&A's) komen. De AFM verwacht dat de ondernemingen reeds aan de slag zijn met het implementeren van DORA om op tijd aan deze regelgeving te voldoen.

In het onderzoek heeft de AFM een aantal observaties gedaan ten aanzien van de monitoring bij uitbesteding van ICT die te weinig aandacht kregen. Omdat deze punten wezenlijke impact kunnen hebben op de beheersing van de bedrijfsvoering, zijn deze observaties opgenomen in dit rapport en worden deze hieronder toegelicht.

Observatie 1 - ICT-kennis binnen ondernemingen was soms onvoldoende

Tijdens het onderzoek constateerde de AFM dat basale kennis over ICT in sommige gevallen ontbrak. Dit brengt extra risico's met zich mee voor de onderneming. De AFM verwacht dat binnen een onderneming personen over passende kennis beschikken, zoals genoemd bij aanbevelingen 6 en 9. Hierbij kan in elk geval worden gedacht aan kennis van ICT-risicomanagement en informatiebeveiliging. Dit geldt ook bij ICT die door derde partijen wordt geleverd. ICT-kennis is nodig bij alle betrokkenen, zoals dagelijks beleidsbepalers en de controle- en monitoringsfuncties.

Observatie 2 - ICT-risico's zijn niet altijd volledig meegenomen in de risicoanalyse

Bij uitbestede werkzaamheden is vaak sprake van de inzet van ICT-middelen. Het bleek dat de bijbehorende ICT-risico's niet altijd volledig meegenomen waren in de risicoanalyse van de onderneming. De AFM wijst erop dat adequaat inzicht in de werkzaamheden van de dienstverlener belangrijk is om de ICT-componenten en de bijbehorende gegevensverwerking te identificeren. Vervolgens is het belangrijk dat ondernemingen, in aanvulling op aanbeveling 5, bij de risicoanalyse expliciet stilstaan bij specifieke ICT-risico's, zoals de risico's rondom de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte gegevens.

Observatie 3 - Verantwoordelijkheid voor informatiebeveiliging niet altijd duidelijk belegd

Uit het onderzoek van de AFM bleek dat ondernemingen ervan uitgaan dat de verantwoordelijkheid voor informatiebeveiliging vaak (gedeeltelijk) bij de dienstverlener hoort. Zij treffen in die gevallen geen of weinig eigen beheersmaatregelen. De onderneming blijft echter zelf eindverantwoordelijk voor haar informatiebeveiliging. Het is van belang dit te laten terugkomen in de schriftelijke procedures en de overeenkomst met de dienstverlener.

Op basis van de uitgevoerde risicoanalyse kan de onderneming een passend beschermingsniveau vaststellen voor de verwerkte gegevens. Zoals genoemd in aanbeveling 10 is het van belang om afspraken te maken met de dienstverlener over de benodigde beheersmaatregelen en hoe deze gemonitord kunnen worden. Stel daarbij ook vast welke beheersmaatregelen door de onderneming zelf ingericht en gemonitord moeten worden. Een voorbeeld is dat een dienstverlener kan zorgdragen voor de technische implementatie van identiteits- en toegangsbeheer in een ICT-systeem, maar dat de onderneming zelf wijzigingen van toegangsrechten goedkeurt en periodiek controleert.

Het is dus van belang dat de taakverdeling tussen de onderneming en de dienstverlener van beheersmaatregelen met betrekking tot ICT duidelijk is en duidelijk is vastgelegd. Hoe de taakverdeling er uit ziet hangt af van het type dienst en het passend beschermingsniveau op basis van de bijbehorende risicoanalyse.

Observatie 4 - Informatiebronnen voor monitoring van ICT-uitbesteding worden niet altijd gebruikt

Voor ICT-uitbestedingen is het van belang dat ondernemingen de prestaties en capaciteit van de uitbestede ICT-componenten zelf bewaken. Een aanzienlijk deel van de ondernemingen ontvangt (geautomatiseerde) rapportages of heeft toegang tot dashboards van de dienstverlener. Dit zijn belangrijke informatiebronnen om de kwantitatieve KPI's te monitoren. Zo kunnen er tijdig maatregelen genomen worden in overleg met de dienstverlener om de beschikbaarheid en veiligheid van de systemen te garanderen, zoals het tijdig opschalen van de capaciteit.

Observatie 5 - Er worden onvoldoende afspraken gemaakt over impactvolle wijzigingen van ICT

Uit het onderzoek blijkt dat niet alle ondernemingen afspraken hebben gemaakt over de wijze waarop wordt omgegaan met impactvolle wijzigingen door de dienstverlener, zoals onderuitbesteding, patches en upgrades van systemen. Impactvolle wijzigingen kunnen risico's met zich meebrengen ten aanzien van de kwaliteit en continuïteit van de dienstverlening. Om deze risico's te kunnen monitoren is het belangrijk om contractuele afspraken te maken met de dienstverlener over de wijze waarop de onderneming geïnformeerd wordt bij impactvolle wijzigingen die de uitbestede ICT-dienst raken. Zo kan de kwaliteit en de continuïteit van de dienstverlening pro-actief gemonitord worden en kunnen er eventuele voorzorgmaatregelen getroffen worden.

Observatie 6 - Er wordt onvoldoende gebruik gemaakt van verslagen over het testen van weerbaarheid

Voor periodieke monitoring van hun ICT-risico's maakt een deel van de ondernemingen gebruik van penetratietesten. Penetratietesten zijn bedoeld om de effectiviteit van informatiebeveilings-maatregelen in de praktijk te kunnen toetsen. Tijdens een dergelijke test wordt gekeken of er kwetsbaarheden in ICT-systemen of applicaties te vinden zijn. Vervolgens worden deze kwetsbaarheden gebruikt om toegang te verkrijgen tot deze systemen. In veel gevallen zullen dienstverleners deze testen reeds uitvoeren of laten uitvoeren door een onafhankelijke partij. Als interne of externe penetratietesten ontbreken, kunnen onderneming afspraken maken met de dienstverlener om deze testen te laten uitvoeren. In dit kader kan het relevant zijn om afspraken te maken over het type testen, de reikwijdte, de frequentie en de uitvoerder (intern of extern).

Penetratietesten zijn een nuttig middel om de continuïteit van de dienstverlening te borgen en daarmee de risico's van uitbesteding effectief te beheersen. Toepassing van de voorschriften van DORA vanaf 17 januari 2025, brengt voor veel ondernemingen de verplichting met zich mee om hun digitale operationele weerbaarheid te testen.

4. Tot slot

De AFM constateert in haar onderzoek dat ondernemingen monitoring op hun uitbestedingen hebben ingericht en in de praktijk brengen. Wel gebruiken ondernemingen regelmatig op onderdelen uitgangspunten die ertoe leiden dat de uitbestedingsrisico's onvoldoende beheerst worden. Dit komt terug in de vijf bevindingen die in dit rapport zijn benoemd. Zo hebben ondernemingen soms geen consequent proces ingericht om tot een juiste conclusie te komen wat wel en niet onder de wettelijke uitbestedingsregels valt. Ook wordt bij de inrichting regelmatig onvoldoende voorgesorteerd op de monitoring en ontbreekt soms een consistente en uitlegbare aanpak op grond van risico's. Ook wordt soms niet goed omgegaan met specifieke situaties, in het bijzonder uitbesteding binnen de groep en ICT-uitbesteding.

De AFM heeft handvatten opgesteld voor de beheersing van de uitbestedingsrisico's. Zij verwacht dat ondernemingen de aanbevelingen in dit rapport meenemen bij de doorlopende beheersing van uitbesteding.

Bijlage I: Aanbevelingen

1. Stel schriftelijk beleid op waarin is uitgewerkt hoe op een eenduidige wijze wordt vastgesteld of sprake is van uitbesteding.
2. Leg in de schriftelijke procedures vast hoe wordt vastgesteld welke werkzaamheden gezien worden als materieel. Hanteer daarbij een niet te nauwe interpretatie van deze begrippen.
3. Stel schriftelijke procedures op waarin per uitbestedingsrelatie wordt uitgewerkt hoe uitbestedingsrisico's geïdentificeerd en beheerst worden.
4. Houd een integraal overzicht bij, met daarin een aantal essentiële elementen van alle uitbestedingsrelaties die zijn aangegaan.
5. Voer zowel ex-ante als ten minste jaarlijks een risicoanalyse uit. Stel daarna voor iedere uitbesteding vast welke beheersmaatregelen passen bij de uitbesteding.
6. Beleg de (eind)verantwoordelijkheid voor de uitbestedingsrelatie en de monitoringsactiviteiten bij specifieke personen, die beschikken over passende kennis en ervaring. Zorg voor een duidelijke taakverdeling binnen het bestuur, met aandacht voor onder wie welke uitbesteding valt.
7. Maak contractuele afspraken waarin is vastgelegd op welke wijze de dienstverlening wordt gemeten, wie daarvoor verantwoordelijk is, welke onderwerpen minimaal in de rapportage worden opgenomen en wat de rapportagefrequentie is.
8. Richt een escalatiestructuur in met escalatiemogelijkheden op verschillende niveaus en, indien relevant, voor zowel operationele functies, als tweedelijnsfuncties.
9. Wijs ook in geval van uitbesteding taken en verantwoordelijkheden toe aan operationele functies ('eerste lijn') en controlefuncties ('tweede en derde lijn') voor het monitoren van de uitbestedingsrelatie (3 LoD).
10. Houd een centraal control framework bij waarin de beheersmaatregelen worden vastgelegd.
11. Monitor de uitbesteding door middel van zowel kwantitatieve als kwalitatieve KPI's en gebruik daarbij rapportages met een passende frequenties.
12. Review beschikbare audit rapportages van derde partijen periodiek op de geldigheid, scope, diepgang en bevindingen van deze rapporten.
13. Stel een helder en gedocumenteerd incidentenprocedure op met betrekking tot incidenten bij dienstverleners.
14. Neem bij intra-groep uitbesteding in het schriftelijke beleid mee dat personele ondersteuning vanuit groepsentiteiten vaak als uitbesteding kwalificeert. Gebruik daarnaast de juiste beheersmaatregelen.
15. Zorg ook bij intra-groep uitbesteding voor passende beheersmaatregelen, die aansluiten bij de intra-groep praktijken en risico's die daaruit voortvloeien.
16. Leg ook bij intra-groep uitbestedingen de afspraken met betrekking tot de monitoring van intra-groep uitbesteding vast in een contract.
17. Maak een schriftelijke analyse specifiek ten aanzien van intra-groep belangenconflicten en leg deze vast.
18. Stel een gedocumenteerd proces op rondom duale functies (dubbele petten) en daarmee samenhangende potentiële belangenconflicten.
19. Leg de eigen verantwoordelijkheden van de monitoringsactiviteiten vast als een groepsentiteit tevens (gedeeltelijk) de monitoring van de (intra-groep) uitbesteding uitvoert.
20. Zorg er voor dat er tot op niveau van het bestuur van de onderneming kan worden geëscaleerd.

Bijlage II: Stroomschema uitbesteding

Deze bijlage bevat een aantal gezichtspunten die naar opvatting van de AFM relevant zijn bij de vaststelling of een opdracht van een onderneming aan een derde om bepaalde werkzaamheden te verrichten (bijvoorbeeld door middel van 'shared services', inleenconstructies, support etc.) kwalificeert als uitbesteding binnen de reikwijdte van de uitbestedingsregels. Deze gezichtspunten laten zich, vereenvoudigd weergegeven, samenvatten zoals in onderstaand stroomschema. Deze gezichtspunten en onderstaand schema zijn uitdrukkelijk bedoeld als handreiking en kunnen geen volledig recht doen aan de verscheidenheid van arrangementen die mogelijk als uitbesteding kwalificeren. Ondernemingen blijven zelf verantwoordelijk voor een juiste kwalificatie van hun uitbestedingen.

De AFM merkt voor de volledigheid op dat, ook voor werkzaamheden die de onderneming door derde partijen laat verrichten en die niet als uitbesteding binnen de reikwijdte van de uitbestedingsregels kwalificeren, ondernemingen verplicht zijn voldoende beheersmaatregelen te treffen om een beheerste bedrijfsvoering te waarborgen.

Of er sprake is van wettelijke uitbesteding en wat daarvan de gevolgen zijn, hangt af van het toepasselijke wettelijk kader. Allereerst dient de onderneming dus vast te stellen welke wet- en regelgeving inzake uitbesteding van toepassing is. Dit is bijvoorbeeld relevant voor beheerders ingeval van een uitbesteding van een kernactiviteit, waarbij de beheerder tevens werkzaamheden laat uitvoeren door derde partijen (al dan niet binnen de groep) die betrekking hebben op de tweede kernactiviteit. Het uitbesteden van twee kernactiviteiten door beheerders is immers niet toegestaan.

Figuur 2. Stroomschema uitbesteding

Eigen werkzaamheden

Ondernemingen kunnen alleen eigen werkzaamheden uitbesteden. Werkzaamheden die een onderneming (juridisch) niet zelf uit mag voeren kunnen dus ook niet worden uitbesteed. Denk hierbij aan de diensten van de bewaarder, externe audit- en brokerdiensten (voor zover dit niet binnen de vergunning past). Dat werkzaamheden nieuw zijn en daarom niet eerder door de onderneming zelf zijn verricht, doet niet af aan het feit dat zulke nieuwe werkzaamheden behoren tot de eigen werkzaamheden van de onderneming.

Materiële werkzaamheden

Uitbestedingen van werkzaamheden die vallen binnen de reikwijdte van de uitbestedingsregels in het relevante wettelijk kader worden in dit rapport aangeduid als materieel, zoals ook toegelicht bij voetnoot 3 in dit rapport. Materiële werkzaamheden zijn volgens artikel 1:1 Wet op het Financieel toezicht werkzaamheden die voortvloeien uit het uitoefenen van het bedrijf of het verlenen van financiële diensten, of op werkzaamheden die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan.

De term wezenlijk in de Wft is een materialiteitsgrens en kan worden vertaald naar verschillende Europese wetgeving. Zo staat in overweging 82 van de Gedelegeerde Verordening (EU) No 231/2013 dat: *"De delegatiebeperkingen en vereisten moeten gelden voor de beheertaken die zijn omschreven in bijlage I van Richtlijn 2011/61/EU, terwijl ondersteunende taken zoals administratieve of technische taken ter ondersteuning van de beheertaken zoals logistieke steun in de vorm van schoonmaak, catering en inkoop van basisdiensten of basisproducten, niet geacht mogen worden delegatie van abi-beheerderstaken in te houden. Andere voorbeelden van technische of administratieve taken zijn het kopen van standaardsoftware „uit voorraad" en het inschakelen van softwareaanbieders voor operationele ad-hoc bijstand met betrekking tot uit voorraad geleverde systemen of het verstrekken van human resources-ondersteuning zoals aantrekken van tijdelijke werknemers of loonadministratie."*

Dit betekent dat taken ter ondersteuning, zoals genoemd in de tekst, niet gezien moeten worden als materieel en daarmee dus niet kwalificeren als uitbesteding in de zin van de uitbestedingsregels.

Binnen het MiFID II kader is dit vereiste terug te vinden onder het 'kritiek en belangrijk'-criterium, zoals opgenomen in artikel 16, vijfde lid, eerste alinea, MiFID II en verder uitgewerkt in artikel 30 van de MiFID II Gedelegeerde Verordening (EU) 2017/565.

Overeenkomst

Wanneer er een arbeidsovereenkomst wordt aangegaan met de persoon die de werkzaamheden uitvoert is er in beginsel geen sprake van een uitbesteding, de persoon werkt dan immers voor de onderneming zelf. Elke andere vorm van een overeenkomst kan leiden tot een uitbesteding. Daarbij zijn de gezichtspunten onder 4, 5 en 6 relevant. Eenmalige dienstverlening valt echter eerder onder ondersteuning (zie punt 2) en wordt over het algemeen niet gezien als uitbesteding.

Specifieke bepalingen

Wanneer het contract specifieke bepalingen bevat ten aanzien van de individuen die de desbetreffende werkzaamheden voor de onderneming verrichten, is dit een indicatie dat er in de praktijk geen sprake is van uitbesteding. In dit geval zijn de gezichtspunten 5 en 6 relevant. Deze specifieke bepalingen zien dan bijvoorbeeld op de specifieke werkzaamheden, het aantal uren, vakantiedagen, beoordelingsgesprekken e.d. per individu. Als het contract geen specifieke bepalingen ten aanzien van deze individuen bevat is dit een teken dat er sprake is van een uitbesteding.

Rapportagelijnen

Als de onderneming controle heeft over de werkzaamheden en prestaties van de individuen die de werkzaamheden verrichten werken zij in principe onder verantwoordelijkheid van de onderneming. In dat geval is er waarschijnlijk geen sprake van uitbesteding. Dit is duidelijk het geval als de individuen die de werkzaamheden verrichten enkel een rapportagelijn hebben binnen de onderneming zelf. Als de individuen alleen een rapportagelijn hebben aan personen binnen de dienstverlener is dat een indicatie dat er sprake van uitbesteding. Soms is er een duale rapportagelijn, in dat geval is het volgende gezichtspunt relevant.

Tijd, toegang en locatie

Als de individuen die de werkzaamheden voor de onderneming verrichten volledig werkzaam zijn voor de onderneming, is de controle groter. Dat is een indicatie dat er geen sprake is van een uitbesteding. Hetzelfde geldt voor de toegang tot systemen voor de individuen die werkzaamheden voor de onderneming uitvoeren en de locatie waar deze individuen de werkzaamheden uitvoeren. Wanneer deze individuen volledig werkzaam zijn op het kantoor van de onderneming of meegaan in het thuiswerkbeleid dat voor alle werknemers van de onderneming geldt en werken met de ICT van de onderneming of zal er minder snel sprake zijn van uitbesteding.

Bijlage III: Juridisch kader

Het juridisch kader is (geüpdatet) overgenomen uit de sectorbrief van Keten in Beeld uit 2019.

Bij uitbesteding van werkzaamheden aan een derde dienen beheerders en beleggingsondernemingen zich te houden aan Nederlandse en Europese wet- en regelgeving. Deze regels zien ook op de monitoring van uitbesteding. Ook zijn er diverse richtsnoeren van toepassing. Deze zijn uitgewerkt in onderstaand overzicht per sector.

Tabel 1. Type financiële onderneming

Artikelen uit wettelijk kaders die zien op uitbesteden	Beleggingsonderneming	Beheerder van een beleggingsinstelling	Beheerder van een icbe
Wet op het Financieel toezicht (Wft)	4:16, lid 1,3	4:16, lid 1-3	4:16, lid 1-3
Besluit Gedragstoezicht financiële ondernemingen Wft (Bgfo)	37	37 37a	37 38 38a
Richtlijn 2011/61/EU (AIFMD-richtlijn) inzake beheerders van alternatieve beleggingsinstellingen	Niet van toepassing	20	Niet van toepassing
Gedelegeerde verordening (EU) 231/2013 (AIFMD-verordening) tot aanvulling van richtlijn 2011/61/EU	Niet van toepassing	75-82	Niet van toepassing
Richtlijn 2014/65/EU (MIFID II-richtlijn) betreffende markten voor financiele instrumenten	16, lid 5 eerste alinea	Niet van toepassing	Niet van toepassing
Gedelegeerde verordening (EU) 2017/565 (MIFID II-verordening) tot aanvulling van richtlijn 2014/65/EU	30-32	Niet van toepassing	Niet van toepassing
Gedelegeerde verordening (EU) 2017/589 (MIFID II-verordening) tot aanvulling van richtlijn 2014/65/EU met organisatorische vereisten voor beleggingsondernemingen die zich met algoritmische handel bezighouden	2, lid 3 4	Niet van toepassing	Niet van toepassing
ESMA richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten, 10 mei 2021, ESMA50-164-4285	Volledig van toepassing	Volledig van toepassing	Volledig van toepassing
EBA richtsnoeren inzake uitbesteding, 25 februari 2019, EBA/GL/2019/02	Beleggingsondernemingen klasse 1	Niet van toepassing	Niet van toepassing
Richtsnoeren met betrekking tot bepaalde aspecten van de MiFID II eisen voor de compliance functie, 6 april 2021, ESMA35-36-1952	Volledig van toepassing	Niet van toepassing	Niet van toepassing

Uit de tabel kan worden opgemaakt dat de uitbestedingsregels voor bijvoorbeeld een beheerder van een icbe minder gedetailleerd zijn uitgewerkt dan bijvoorbeeld de regels voor een beheerder van een beleggingsinstelling. En, na een analyse van de regels, dat de regels voor bijvoorbeeld beheerders van een beleggingsinstelling anders zijn dan de regels voor bijvoorbeeld een beleggingsonderneming. Hierdoor zou de indruk kunnen ontstaan dat uitbestedingsregels minder (of meer) omvatten afhankelijk van het type financiële onderneming.

De AFM is van mening dat alle uitbestedingsregels die zijn opgenomen in bovenstaande regelingen betekenis hebben voor ondernemingen. De AFM is namelijk van oordeel dat de regelingen – ondanks afwijkingen in de uitwerking – in beginsel allemaal hetzelfde doel dienen: de beheersing van uitbestedingsrisico's door ondernemingen. Ongeacht de financiële dienst die een onderneming verleend, een onderneming blijft verantwoordelijk voor de werkzaamheden die zij uitbesteedt, zowel richting haar toezichthouder als haar klanten, en van een onderneming wordt verwacht "in control" te zijn. Dit betekent, ter illustratie, dat wanneer een onderneming twijfelt hoe beheersmaatregelen het beste kunnen worden ingericht volgens de regeling die op haar van toepassing is, de regels uit een andere regelingen mogelijk praktische diepgang kan bieden.

Bovendien komen de regelingen op belangrijke punten overeen. Een voorbeeld hiervan is dat werkzaamheden alleen kunnen vallen onder de wettelijke definitie van uitbesteden wanneer deze werkzaamheden zien op de "normale" taken van een onderneming (zie bijlage IV). De AFM ziet in de verschillende regels dan ook belangrijke aandachtspunten die consistent door ondernemingen kunnen worden toegepast om hen te helpen om in control te zijn en te blijven met betrekking tot uitbesteden. Aanvullend merkt de AFM daarbij op dat diverse aandachtspunten ook kunnen worden gebruikt buiten het kader van uitbesteden: immers ook wanneer een onderneming werkzaamheden inkoopt of simpelweg met derde partijen samenwerkt, dient een onderneming in control te zijn op grond van artikel 4:14 Wft.

Bijlage IV: Sectorbrief Keten in Beeld 2019, onderdeel "beoordelen uitbesteden"

Definitie uitbesteden en "normale taken"

Ondernemingen moeten vaststellen of werkzaamheden die worden uitgevoerd door een derde partij vallen onder uitbesteden.

Uitbesteden wordt in de wet als volgt gedefinieerd:

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;*

Voor specifiek beleggingsondernemingen geldt een afwijkende definitie:

een overeenkomst van om het even welke vorm tussen een beleggingsonderneming en een dienstverlener op grond waarvan deze dienstverlener een proces, een dienst of een activiteit verricht die anders door de beleggingsonderneming zelf zou worden verricht

Ondanks de afwijkende woorden in bovenstaande definities, geldt in beginsel voor alle ondernemingen dat uitbesteden ziet op werkzaamheden die een onderneming door een derde partij laat verrichten en die anders door de onderneming zelf worden verricht. Werkzaamheden die een onderneming zelf moet verrichten vallen onder haar takenpakket. Hierbij geldt dat werkzaamheden verschillende kenmerken kunnen hebben. Werkzaamheden kunnen bijvoorbeeld zien op individuele of een reeks aan werkzaamheden en ze kunnen eenmalig of doorlopend worden verricht. Daarnaast kan het zijn dat een onderneming werkzaamheden uitbesteedt die zien op nieuwe werkzaamheden, waardoor de onderneming de werkzaamheden niet eerder zelf heeft verricht. Daarnaast kunnen de werkzaamheden geconcentreerd binnen een afdeling of een functie worden uitgevoerd, zoals bijvoorbeeld de verzameling van werkzaamheden die worden uitgevoerd door (/binnen) de compliance afdeling (/functie). Wanneer een onderneming werkzaamheden laat verrichten door een derde partij, welke tot haar eigen takenpakket behoort, dan kan er sprake zijn van uitbesteden. In het verdere verloop van deze brief worden de werkzaamheden die tot het takenpakket van een onderneming behoren gevat onder de term 'normale taken'.

Tabel 2 geeft een overzicht van normale taken met betrekking tot de drie verschillende type financiële ondernemingen. Ieder van deze taken bestaat uit een diversiteit aan werkzaamheden, waarvoor in beginsel geldt dat wanneer een onderneming een of meerdere werkzaamheden laat verrichten door een derde partij dit altijd valt onder de definitie uitbesteden. Er gelden echter algemene en specifieke uitzonderingen.

Tabel 2. Normale taken

Taken	**Beleggingsonderneming** (MIFID II-richtlijn artikel 16, lid 5 eerste alinea)	**Beheerder van een beleggingsinstelling** (AIFMD-richtlijn bijlage I)	**Beheerder van een icbe** (UCITS-richtlijn bijlage II)
1	Kritieke of belangrijke taken ("kerntaken")	Portefeuillebeheer	Beheer van beleggingen
2	Overige taken	Risicobeheer	
3		Administratie, waaronder de volgende werkzaamheden worden verstaan: • Uitvoeren van de wettelijk verplichte en voor het fondsbeheer vereiste werkzaamheden op het gebied van de verslaglegging; • Verzoeken om inlichtingen van cliënten; • Waardering en prijsstelling (met inbegrip van belastingaangiften); • Toezien op de naleving van de regelgeving; • Bijhouden van een deelnemersregister; • Bestemming van de inkomsten; • Uitgifte en inkoop van rechten van deelneming; • Afwikkeling van contracten (met inbegrip van de verzending van deelbewijzen); • Bijhouden van bescheiden.	
4		Verhandeling	
5		Werkzaamheden met betrekking tot de activa van de beleggingsinstelling	

Algemene uitzonderingen

Iedere onderneming geeft een unieke invulling aan haar bedrijfsvoering, bedrijfsprocessen en financiële diensten. Vandaar dat dezelfde type ondernemingen (met dezelfde financiële dienstverlening) weliswaar vergelijkbare normale taken hebben, maar toch afwijkende werkzaamheden kunnen verrichten. Een algemeen overzicht van werkzaamheden die vallen onder uitbesteden is daarom niet mogelijk. Wel zijn er uitzonderingen die in het algemeen van toepassing zijn op de verschillende type ondernemingen. Onderstaande algemene uitzonderingen kunnen een onderneming helpen in haar beoordeling welke werkzaamheden, welke worden uitgevoerd door een derde partij, in de regel niet vallen onder uitbesteden:

- werkzaamheden die (wettelijk) alleen door een dienstverlener kunnen worden verricht, zoals bijvoorbeeld de verplichte controle van de jaarrekening door een accountant, het in bewaring geven van gelden en financiële instrumenten bij een depotbank of de uitvoering van orders in financiële instrumenten door een broker
- verlening van advies die geen onderdeel vormen van de normale taken van een onderneming, zoals bijvoorbeeld (juridische) adviezen. Hieruit volgt dat bijvoorbeeld adviezen die zien op arbeidsrechtelijke zaken in de regel niet zullen vallen onder uitbesteden, maar compliance adviezen die vrijwel 1-op-1 worden overgenomen en daarmee een gehele of gedeeltelijke invulling geven aan de compliance functie wel degelijk kenmerken hebben van uitbesteden. Een ander voorbeeld dat kenmerken heeft van uitbesteden zijn beleggingsadviezen of adviezen die zien op de ontwikkeling van modelportefeuilles die (in praktijk) 1-op-1 worden overgenomen in een beleggingsportefeuille.
- verlening van andere diensten die geen onderdeel vormen van de normale taken van een onderneming, zoals bijvoorbeeld de catering, de schoonmaak of de opleiding van personeel
- de aankoop van gestandaardiseerde diensten, zoals bijvoorbeeld koers- en marktinformatiediensten

De AFM merkt in dit kader op dat het niet ongebruikelijk is dat dienstverleners meerdere werkzaamheden combineren en aanbieden als integraal dienstverleningspakket. Een eerste voorbeeld hiervan is een aangestelde depotbank of custodian die naast bewaarnemingstaken (niet uitbesteden) ook compliance en administratieve werkzaamheden (mogelijk wel uitbesteden) verrichten voor een onderneming. Een tweede voorbeeld is (een leverancier van) een portefeuille beheersysteem (niet uitbesteden), waarin feitelijk de gehele of gedeeltelijke risicobeheerfunctie en klantenrapportage (mogelijk wel uitbesteden) van een onderneming is verwerkt. Deze voorbeelden tonen aan dat het mogelijk is dat een derde partij een reeks aan werkzaamheden verricht, die gedeeltelijk onder de normale taken van een onderneming vallen.

Dit betekent dat een deel van de werkzaamheden in deze voorbeelden niet en andere (wanneer het normale taken betreft) mogelijk wel onder de uitbestedingsregels vallen.

De AFM acht het van belang dat uw onderneming doorlopend een volledig beeld heeft welke werkzaamheden uw onderneming uitbesteedt, waaronder werkzaamheden die wellicht (reeds langere tijd) zijn geïntegreerd in de bredere dienstverlening van een derde partij.

Specifieke uitzonderingen

Voor bepaalde ondernemingen gelden specifieke uitzonderingen. Onderstaand worden deze uitzonderingen toegelicht per type financiële onderneming.

Beleggingsondernemingen

Voor beleggingsondernemingen geldt dat werkzaamheden waarop uitbestedingsregels van toepassing zijn worden gevat onder de beschrijving "kritieke of belangrijke" taken (kerntaken – zie tabel 2). Dit betekent dat wanneer werkzaamheden niet vallen onder de kerntaken van een onderneming, deze formeel niet vallen onder de uitbestedingsregels.

Het is daarom specifiek voor een beleggingsonderneming van belang dat wordt beoordeeld welke werkzaamheden vallen onder haar kerntaken. Wederom geldt hier dat vanwege een unieke invulling van de bedrijfsvoering per onderneming, een algemeen overzicht van kerntaken niet kan worden gegeven. Wel kunnen beleggingsondernemingen worden geholpen met haar beoordeling, omdat werkzaamheden met de volgende kenmerken altijd vallen onder haar kerntaken:

Werkzaamheden waarbij een gebrekkige of tekortschietende uitvoering wezenlijk nadelige gevolgen heeft voor de onderneming op het gebied van:

a. haar plicht om doorlopend te voldoen aan de algemene of onderneming-specifieke vergunningsverplichtingen
b. haar financiële resultaten
c. de soliditeit of continuïteit van de beleggingsdienstverlening of -activiteiten

Werkzaamheden die zien op de interne controlefunctie van de onderneming

Werkzaamheden die zien op taken van de onderneming waarvoor een vergunning is vereist

De AFM wil benadrukken dat, ondanks dat uitbestedingsregels alleen van toepassing zijn bij uitbesteden van kerntaken, de beheersmaat-regelen en aandachtspunten die later in deze brief worden genoemd ondernemingen ook kunnen helpen in control te zijn met betrekking tot het uitbesteden van "overige taken" (zie tabel in deze bijlage).

Beheerder van een beleggingsinstelling

Twee functies die een beheerder van een beleggingsinstelling op zijn minst moet verlenen, zijn portefeuille- en risicobeheer (zie tabel 2). Een beheerder kan besluiten om de werkzaamheden die één van de functies omvat, uit te besteden. Het is een beheerder echter niet toegestaan om de werkzaamheden die zien op beide functies uit te besteden.

De overige functies die een beheerder van een beleggingsinstelling kan uitoefenen (zie tabel 2) vallen in beginsel onder de normale taken van een beheerder. Bepaalde onderdelen zijn echter niet op alle beheerders van beleggingsinstellingen van toepassing. Een voorbeeld hiervan is een beheerder van bijvoorbeeld een "closed-end" fonds die geen taken zal verrichten die zien op de inkoop van rechten van deelneming. Een ander voorbeeld is een beheerder van bijvoorbeeld een aandelenfonds die waarschijnlijk geen taken zal verrichten met betrekking tot de activa van de beleggingsinstelling. Uiteraard geldt dat wanneer taken niet van toepassing zijn, en dus niet vallen onder de normale taken van een onderneming, er ook geen sprake kan zijn van uitbesteding.

Beheerder van een icbe

Voor een beheerder van een icbe zijn er geen specifieke uitzonderingen. Voor deze beheerders geldt de algemene definitie van uitbesteden en zijn de algemene uitzonderingen van toepassing.