Uitbesteding aan Blanco

Beleggingsondernemingen

Augustus 2021

Inhoud

1. Inleiding

Uitbesteding is een belangrijk onderwerp, zowel voor u in de dagelijkse praktijk, als in de ogen van de toezichthouders. In de sectorbrief van november 2019 schreef de AFM:

> *"Uitbesteden van werkzaamheden vindt veel plaats en volgt in de regel uit een streven naar een efficiëntere bedrijfsvoering door een onderneming. Uitbesteden kan bijvoorbeeld bijdragen aan een verbetering van de kwaliteit en/of een verlaging van de kosten van de dienstverlening. Uitbesteden brengt echter ook risico's met zich mee. Ondernemingen dienen te zorgen dat de risico's die volgen uit uitbesteden worden beheerst, ongeacht de reden om werkzaamheden uit te besteden. De kern van uitbestedingsrisico's ligt in het feit dat een onderneming niet zelf de werkzaamheden verricht, maar wel zelf verantwoordelijk blijft voor deze werkzaamheden. De verantwoordelijkheid (en daarmee eventueel de aansprakelijkheid) kan niet worden overgedragen aan een derde partij.*
>
> *Een onderneming kan het risico dat een derde partij de werkzaamheden niet of van onvoldoende kwaliteit uitvoert alleen mitigeren door (doorlopende) controle te houden over deze werkzaamheden. Dit betekent dat van een onderneming wordt verwacht dat zij 1) volledig inzicht heeft in alle werkzaamheden die worden uitgevoerd door derde partijen, 2) kennis heeft over alle uitbestedingsregels die op haar van toepassing zijn en 3) de nodige maatregelen heeft getroffen om de risico's die volgen uit het uitbesteden te beheersen."*

Omdat Blanco en AIRS (hierna samen 'Blanco' genoemd) graag goede uitbestedingspartners willen zijn, vinden wij het niet meer dan logisch om u enige ondersteuning te bieden bij uw uitbestedingen. Graag willen wij u met dit 'Blanco-paper' wat tekst en toelichting geven over uw (algemene) verplichtingen en de manier waarop Blanco u kan helpen hieraan te voldoen bij uitbesteding aan Blanco.

We beseffen ons dat de omvang van het document niet echt uitnodigend is, maar helaas is uitbesteding een omvangrijk onderwerp waarover het nodige geschreven is. We hebben deze informatie zo goed mogelijk voor u proberen te structureren, zodat het wellicht makkelijker wordt u een weg te banen door alle publicaties die beschikbaar zijn.

2. Wet- en regelgeving

2.1. Uitbesteding ja of nee?

Laten we beginnen bij het begin. Als beleggingsonderneming dient u zich te houden aan de uitbestedingsregels zoals opgenomen in MiFID II (en geïmplementeerd in de nationale wetgeving). Maar om te bepalen of u aan de uitbestedingsregels moet voldoen, is het belangrijk om eerst te bepalen wanneer er eigenlijk sprake is van uitbesteding zoals bedoeld in de wet.

Er is sprake van uitbesteding indien kritieke en belangrijke operationele taken van een beleggingsonderneming worden uitgevoerd door een derde partij. Het gaat daarbij om een overeenkomst tussen de beleggingsonderneming en een derde partij op grond waarvan de derde partij een proces, dienst of activiteit verricht die anders door de beleggingsonderneming zelf zou worden verricht. Als voorbeeld: het in bewaring geven van gelden en financiële instrumenten bij een depotbank is geen uitbesteding, omdat dit proces (in de meeste gevallen) geen onderdeel uitmaakt van uw eigen vergunning. Dit

wordt tevens door de AFM bevestigd. Maar let op! Als uw depotbank ook nog andere diensten levert, is er mogelijk wél sprake van uitbesteding. Daarnaast staan in de wet ook voorbeelden van taken die niet als uitbesteding kwalificeren, zoals juridisch advies en de aankoop van koersinformatiediensten. Het gebruik van een portfolio management systeem kwalificeert bijvoorbeeld weer wél als uitbesteding. Het verdient dus aanbeveling om kritisch te kijken naar de partijen die u gebruikt en per partij vast te stellen of de dienstverlening kwalificeert als uitbesteding, als inkoop of als een samenwerking.

2.2. Wettelijke eisen

Indien u heeft vastgesteld dat er inderdaad sprake is van uitbesteding als bedoeld in de wet, dan dient u te voldoen aan de wettelijke eisen die zijn opgenomen in artikel 31 Gedelegeerde verordening MiFID II. Verder in dit document zullen we nader ingaan op deze wettelijke verplichtingen, maar mocht u benieuwd zijn naar de letterlijke tekst van de wettelijke verplicht, dan luidt deze als volgt:

> *1. Beleggingsondernemingen die kritieke of belangrijke operationele taken uitbesteden, blijven volledig verantwoordelijk voor de nakoming van al hun verplichtingen op grond van Richtlijn 2014/65/EU en voldoen aan de volgende voorwaarden:*
>
> *a) de uitbesteding resulteert niet in het delegeren door de directie van haar verantwoordelijkheid;*
> *b) de relatie en verplichtingen van de beleggingsonderneming jegens haar cliënten uit hoofde van Richtlijn 2014/65/EU wordt niet gewijzigd;*
> *c) de voorwaarden waaraan de beleggingsonderneming moet voldoen om overeenkomstig artikel 5 van Richtlijn 2014/65/EU een vergunning te verkrijgen, en deze te behouden, worden niet ondermijnd;*
> *d) geen van de andere voorwaarden waaronder de vergunning aan de onderneming is verleend, worden opgeheven of gewijzigd.*
>
> *2. Beleggingsondernemingen leggen de nodige bekwaamheid, zorgvuldigheid en waakzaamheid aan de dag bij het aangaan, beheren of beëindigen van een overeenkomst voor de uitbesteding van kritieke of belangrijke operationele taken aan een dienstverlener en doen de noodzakelijke stappen om ervoor te zorgen dat de volgende voorwaarden worden vervuld:*
>
> *a) de dienstverlener beschikt over de bekwaamheid, capaciteit, voldoende middelen, een passende organisatiestructuur ter ondersteuning van de uitvoering van de uitbestede taken en elke bij wet vereiste vergunning om de uitbestede taken op betrouwbare en professionele wijze uit te voeren;*
> *b) de dienstverlener voert de uitbestede diensten daadwerkelijk en met inachtneming van de toepasselijke wettelijke en bestuursrechtelijke voorschriften uit, en daartoe heeft de onderneming methoden en procedures ingesteld om het prestatieniveau van de dienstverlener te beoordelen en om doorlopend de door de dienstverlener verleende diensten te toetsen;*
> *c) de dienstverlener houdt afdoende toezicht op de uitvoering van de uitbestede taken en beheert de aan de uitbesteding verbonden risico's op adequate wijze;*
> *d) er wordt passende actie ondernomen mocht blijken dat de dienstverlener de taken niet efficiënt en met inachtneming van de toepasselijke wettelijke en bestuursrechtelijke voorschriften uitvoert;*
> *e) de beleggingsonderneming houdt daadwerkelijk toezicht op de uitbestede taken of diensten en beheert de risico's in verband met de uitbesteding en te*

dien einde behoudt de onderneming de noodzakelijke deskundigheid en middelen om daadwerkelijk toezicht uit te oefenen op de uitbestede taken en die risico's te beheren;

f) *de dienstverlener heeft de beleggingsonderneming in kennis gesteld van elke ontwikkeling die van wezenlijke invloed kan zijn op zijn of haar vermogen om de uitbestede taken efficiënt en met inachtneming van de toepasselijke wettelijke en bestuursrechtelijke voorschriften uit te voeren;*
g) *de beleggingsonderneming kan de uitbestedingsovereenkomst indien nodig met onmiddellijke ingang beëindigen wanneer dit in het belang is van haar cliënten, zonder dat dit nadelige gevolgen heeft voor de continuïteit en de kwaliteit van haar dienstverlening aan cliënten;*
h) *de dienstverlener werkt met betrekking tot de uitbestede taken samen met de bevoegde autoriteiten van de beleggingsonderneming;*
i) *de beleggingsonderneming, haar accountants en de relevante bevoegde autoriteiten hebben effectieve toegang tot de gegevens over de uitbestede taken en tot de relevante bedrijfsruimten van de dienstverlener indien noodzakelijk voor daadwerkelijk toezicht in overeenstemming met dit artikel, en de bevoegde autoriteiten kunnen die toegangsrechten uitoefenen;*
j) *de dienstverlener beschermt alle vertrouwelijke informatie over de beleggingsonderneming en haar cliënten;*
k) *de beleggingsonderneming en de dienstverlener hebben een noodplan vastgesteld, geïmplementeerd en in stand gehouden dat voorziet in calamiteitenbeheersing en in een periodieke controle van de back-upvoorzieningen wanneer dit noodzakelijk is gelet op de uitbestede functie, dienst of activiteit;*
l) *de beleggingsonderneming heeft ervoor gezorgd dat de continuïteit en de kwaliteit van de uitbestede taken of diensten ook in geval van de beëindiging van de uitbesteding gehandhaafd blijven door ofwel de uitbestede taken of diensten aan een andere derde over te dragen, of deze zelf te vervullen;*

3. De respectieve rechten en plichten van de beleggingsonderneming en de dienstverlener zijn duidelijk afgebakend en in een schriftelijke overeenkomst omschreven. De beleggingsonderneming behoudt met name haar instructie- en beëindigingsrechten, haar recht op informatie en haar recht op inspectie en op toegang tot de boeken en bedrijfsruimten. De overeenkomst waarborgt dat uitbesteding door de dienstverlener slechts met schriftelijke toestemming van de beleggingsonderneming plaatsvindt.

4. Indien de beleggingsonderneming en de dienstverlener tot dezelfde groep behoren, mag de beleggingsonderneming voor de naleving van dit artikel en artikel 32 rekening houden met de mate waarin de onderneming zeggenschap heeft over de dienstverlener of invloed kan uitoefenen op diens handelingen.

5. Beleggingsondernemingen stellen desgevraagd de bevoegde autoriteit alle informatie beschikbaar die zij nodig heeft om toezicht te kunnen uitoefenen op de inachtneming bij de vervulling van de uitbestede taken van de vereisten van Richtlijn 2014/65/EU en de uitvoeringsmaatregelen daarvan.

3. Guidelines

Omdat wetgeving vaak risicogebaseerd is, en daarom ruimte laat voor eigen invulling, is het soms lastig te bepalen wanneer u voldoet aan de eisen van de wet. Daarom worden er met enige regelmaat guidelines gepubliceerd door verschillende toezichthouders, zoals EBA, DNB en AFM.

3.1. EBA Richtsnoeren inzake uitbesteding

De EBA heeft in 2019 de finale richtsnoeren over uitbesteding gepubliceerd. De richtsnoeren treft u op de volgende pagina: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements. De richtsnoeren schrijven verschillende governance vereisten voor bij het aangaan van uitbesteding van activiteiten. Het is een zeer omvangrijk stuk, maar kan u helpen een beter beeld te vormen bij wat er van u als beleggingsonderneming kan worden verwacht.

Om het - voor zover mogelijk - u iets makkelijker te maken, hebben wij in Bijlage 1 van dit document een tabel opgenomen met daarin de verschillende richtsnoeren. U kunt deze tabel gebruiken om per richtsnoer aan te geven hoe u compliant bent, of u kunt aangeven dat een bepaald richtsnoer niet op uw situatie van toepassing is. Tevens hebben wij in de tabel waar mogelijk een opmerking gemaakt over hoe Blanco erin kan voorzien dat u met betrekking tot een uitbesteding aan Blanco aan vereisten kunt voldoen.

Overigens is het nog goed te vermelden dat in de richtsnoeren is benadrukt dat ondernemingen rekening moeten (mogen) houden met het evenredigheidsbeginsel.

U kunt de tabel in Word-versie bij ons opvragen.

3.2. ESMA Richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten

ESMA heeft in de zomer van 2021 richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten gepubliceerd. De richtsnoeren treft u op de volgende pagina: https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-providers

Deze richtsnoeren gelden met ingang van 31 juli 2021 voor alle uitbestedingsovereenkomsten betreffende clouddiensten die op of na deze datum van kracht worden, verlengd worden of worden gewijzigd. Ondernemingen moeten bestaande uitbestedingsovereenkomsten betreffende clouddiensten dienovereenkomstig herzien en wijzigen om te zorgen dat zij uiterlijk op 31 december 2022 aan deze richtsnoeren voldoen.

In Bijlage 2 van dit document is ook een tabel opgenomen met daarin de verschillende richtsnoeren van ESMA. U kunt deze tabel gebruiken om per richtsnoer aan te geven hoe u compliant bent, of u kunt aangeven dat een bepaald richtsnoer niet op uw situatie van toepassing is. Tevens hebben wij in de tabel waar mogelijk een opmerking gemaakt over hoe Blanco erin kan voorzien dat u met betrekking tot een uitbesteding aan Blanco aan vereisten kunt voldoen.

U kunt de tabel in Word-versie bij ons opvragen.

4. De verplichtingen

4.1. Beleid

Iedere beleggingsonderneming die werkzaamheden uitbesteedt of voornemens is om werkzaamheden uit te besteden, dient een goed uitbestedingsbeleid te hebben. Conform de richtsnoeren van de EBA dient een uitbestedingsbeleid de levenscyclus van uitbestedingsregelingen te omvatten, met een omschrijving van de beginselen, verantwoordelijkheden en processen in relatie tot de uitbesteding. Zie Bijlage 1, richtsnoer 41 en verder voor meer informatie over het uitbestedingsbeleid.

Ook de AFM heeft in haar recente uitvraag omtrent uitbesteding een indicatie gegeven van de elementen die opgenomen kunnen worden in het uitbestedingsbeleid en/of waar het uitbestedingsbeleid aan moet voldoen:

Het uitbestedingsbeleid...

- is in lijn met de strategie van de organisatie;
- is vastgesteld op senior niveau, door bijvoorbeeld het bestuur of een gedelegeerd functionaris;
- is op groepsniveau gedefinieerd;
- schrijft voor dat voor elke uitbesteding een business case wordt bepaald;
- schrijft voor dat voor elke uitbesteding de eisen aan de leverancier en de dienstverlening zijn vastgesteld;
- schrijft voor dat voor elke uitbesteding besluitvorming op senior niveau plaatsvindt;
- schrijft voor dat voor elke uitbesteding een risico analyse plaatsvindt;
- schrijft voor dat maatregelen getroffen worden om onacceptabele risico's te mitigeren;
- schrijft voor dat compliance betrokken is bij het besluit om uit te besteden;
- schrijft voor dat voor elke uitbesteding wettelijke vereisten geïnventariseerd en gewogen zijn verplicht voorafgaand aan elke uitbesteding een due dilligence onderzoek uit te voeren;
- schrijft voor dat rechten, plichten en verantwoordelijkheden contractueel worden vastgelegd;
- schrijft voor dat contractuele bepalingen vooraf worden getoetst door compliance, JZ en de business;
- schrijft voor dat wettelijke bepalingen zoals right to examine en right to audit zijn opgenomen in uitbestedingsovereenkomsten, indien van toepassing;
- bevat richtlijnen voor de overeen te komen servicelevels;
- bevat richtlijnen voor de overeen te komen rapportages en frequentie van rapportages;
- schrijft voor dat continuïteitsrisico's periodiek worden geïdentificeerd en geëvalueerd;
- schrijft voor dat continuïteitswaarborgen van leveranciers ten minste jaarlijks worden beoordeeld;
- schrijft voor dat voor elke uitbesteding een continuïteitsplan is opgesteld;
- schrijft voor dat in relatie tot continuïteitsrisico's en waarborgen ook onderaannemers in scope worden meegenomen;
- schrijft voor dat de opvolging van wensen en eisen ten aanzien van de dienstverlening periodiek worden beoordeeld;
- schrijft voor dat voor elke uitbesteding periodiek assurance over het stelsel van interne beheersing wordt geleverd;

- schrijft voor dat informatiebeveiliging onderdeel is van de periodieke assurance die de dienstverlener over de geboden dienstverlening levert;
- schrijft voor dat bij elke uitbesteding de onderneming vastlegt dat zij eigenaar is van de data en toegang tot die data geborgd is;
- schrijft voor dat data portabiliteit van de data contractueel is vastgelegd;
- schrijft voor dat de dienstverlener een actueel inzicht in de locatie van de data geeft;
- bevat richtlijnen voor een exit strategie.

Het is belangrijk om het uitbestedingsbeleid regelmatig te evalueren en te updaten, zodat het beleid altijd aansluit op de organisatie van de beleggingsonderneming en de ontwikkelingen in wet- en regelgeving.

4.2. Selectie- en beoordelingsprocedure

Omdat u als beleggingsonderneming zelf verantwoordelijk blijft voor de uitbestede werkzaamheden, dient u uw dienstverleners zorgvuldig te selecteren. Conform de richtsnoeren (nummer 70) van de EBA dient de dienstverlener te beschikken over een aantal eigenschappen. Om u ten aanzien van uw uitbesteding aan Blanco op weg te helpen, geven wij u graag input die u kan helpen de eigenschappen te toetsen. Uiteraard is het daarbij ook aan uzelf om Blanco kritisch te beoordelen en ons extra informatie te vragen indien u dat nodig heeft voor uw beoordeling.

Eigenschap conform EBA-richtsnoeren	Blanco
Een goede reputatie	Blanco beschikt over een goede reputatie. Blanco kent veel tevreden klanten; we zijn dan ook enorm trots op onze hoge retentiescore! Op onze website https://www.useblanco.com zijn enkele testimonials van tevreden klanten te vinden. En wellicht ten overvloede, maar belangrijk om te vermelden: geen van de stakeholders van Blanco (bestuurders, commissarissen, werknemers, investeerders, etc) zijn ooit negatief in de publiciteit gekomen, en hebben allen een goede reputatie.
Passende en toereikende bekwaamheden	Om de perfecte partner te kunnen zijn voor onze vergunninghoudende klanten, is Blanco zelf ook (vrijwel helemaal) ingericht als een gereguleerde onderneming en hebben wij mensen met de juiste specialismen aan boord: gecertificeerde compliance officers, EDP-auditors, privacy professionals en risk experts.
Deskundigheid	Blanco beschikt over ruime ervaring en deskundigheid met betrekking tot de relevante markt. Bij Blanco werken veel mensen met een bancaire achtergrond en/of ervaring in de sector, zodat goed

	met de klant kan worden meegedacht en er geschikte dienstverlening kan worden aangeboden.
De capaciteit	Blanco bouwt schaalbare en innovatieve oplossingen die belangrijke processen binnen een vergunninghoudende organisatie automatiseren. Dat betekent dat er minder handmatig werk hoeft te worden verricht, waardoor er minder personele capaciteit nodig is, zowel bij de klant als bij Blanco zelf. Uiteraard zal Blanco er altijd voor zorgen dat zij over een groot en kundig team beschikt om alle klanten goed te kunnen bedienen.
De middelen (personeel, IT, financieel)	Personeel: Blanco zorgt ervoor dat er altijd voldoende personeel aan boord is om klanten goed te kunnen bedienen. IT: Blanco ontwikkelt en draait in de cloud bij Amazon (AWS). Het grote voordeel hiervan is dat gebruik kan worden gemaakt van de nieuwste technologie en dat de datacapaciteit oneindig schaalbaar is. Financieel: Blanco wordt voor een groot deel gefinancierd door professionele venture capital partijen, zoals KBC Focus Fund, Volta Ventures en Dutch Founders Fund. Zie voor meer informatie: https://www.useblanco.com/about-us#investors
De organisatiestructuur	Blanco houdt bij haar organisatiestructuur rekening met het feit dat haar klanten allen financiële ondernemingen zijn. Blanco heeft dan ook alle relevante disciplines in huis om haar klanten optimaal te kunnen bedienen. Zie voor meer informatie ook: https://www.useblanco.com/governance
Indien van toepassing: de vereiste wettelijke vergunning of registratie.	Niet van toepassing. Blanco verricht zelf geen vergunninghoudende activiteiten.

Ook de AFM heeft in de sectorbrief uit 2019 aangegeven waar aan gedacht moet worden bij het hanteren van een selectieprocedure. Aanvullend op de suggesties van EBA noemt de volgende aandachtspunten:

Aandachtspunten AFM	Blanco
De aanstelling van derde partijen leidt niet tot onbeheersbare concentratierisico's	Omdat Blanco een 'one-stop-shop' is, waarbij verschillende processen binnen uw organisatie kunnen worden ondersteund, zou er mogelijk sprake kunnen zijn van een concentratierisico. Echter, het bestaan van een risico hoeft niet direct een probleem te zijn, mits er goede beheersmaatregelen worden getroffen. Om u te helpen bij de

	onderbouwing van de beheersmaatregelen ten aanzien van dit concentratierisico, hebben wij verderop in het document (en concreet in Bijlage 3) een voorzet gegeven van mitigerende maatregelen.
De derde partij beschikt over adequate technische en organisatorische maatregelen die zien op de bescherming van persoonlijke of vertrouwelijke informatie van de onderneming	Blanco heeft als IT provider en als verwerker van persoonsgegevens uiteraard adequate technische en organisatorische maatregelen ingericht. Kort samengevat heeft Blanco de volgende maatregelen getroffen: • Blanco heeft een beleid en raamwerk voor informatiebeveiliging geïmplementeerd; • Personeel van Blanco wordt gescreend en een geheimhoudingsverklaring maakt onderdeel uit van de arbeidsovereenkomst; • Blanco heeft fysieke en logische toegangscontrole geïmplementeerd. Waar mogelijk wordt tweefactor-authenticatie gebruikt. Bovendien zijn er speciale toegangsbeperkingen; • Blanco heeft een incident- en datalekbeleid en zal de klant onmiddellijk informeren over inbreuken in verband met persoonsgegevens en andere ernstige beveiligingsincidenten; • Blanco is verantwoordelijk voor passende logging en controle van toegang tot persoonsgegevens; • Blanco toetst regelmatig de naleving van het beleid en de kwaliteit van de beveiligingsmaatregelen. Informatiebeveiliging en privacy zijn thema's die in scope zijn van de ISAE3402 van Blanco, en worden dus door een onafhankelijke auditor gecontroleerd. Op verzoek kunnen wij u nadere toelichting geven over de wijze waarop Blanco haar informatiebeveiliging heeft ingericht.
De derde partij gaat een overeenkomst aan waarin duidelijk de rechten en plichten van de onderneming zijn afgebakend, waaronder een waarborg dat de onderneming na uitbesteden doorlopend haar monitorings- en controleverplichtingen kan uitvoeren	Zie het onderwerp 'contract' in dit document voor meer informatie over de overeenkomst van Blanco.

De onderneming heeft methoden en procedures opgesteld om materiële ontwikkelingen bij en het prestatieniveau van de derde partij te beoordelen en doorlopend te toetsen	Het is natuurlijk aan uzelf om het prestatieniveau van Blanco te beoordelen. Blanco heeft in de overeenkomst service levels opgenomen, die u kunnen helpen bij het beoordelen van de dienstverlening.
De onderneming waarborgt dat er voldoende deskundigheid en middelen behouden blijven binnen de onderneming om daadwerkelijk toezicht uit te oefenen op de uitbestede werkzaamheden en om de uitbestedingsrisico's te begrijpen en te beheersen	U dient te waarborgen dat voldoende deskundigheid en middelen behouden blijven. Graag benadrukken we dat we bij Blanco geloven in een symbiose van mens en machine. Onze slimme fintech-oplossingen besparen veel tijd en geld, maar integreren altijd de menselijke factor: onze technologie willen we niet 'van bovenaf' opleggen, maar juist in dienst laten staan van de mens. Dat betekent dat u zelf actief gebruik kunt maken van de software en op die manier direct kunt toezien op de werkzaamheden en (operationele) risico's direct kunt signaleren.
De onderneming waarborgt dat de continuïteit en kwaliteit van de werkzaamheden gehandhaafd blijven bij beëindiging van de uitbesteding door een overdracht van de werkzaamheden aan een derde of deze zelf over te nemen.	De overeenkomst met Blanco bevat een exit-clausule waarin afspraken zijn opgenomen met betrekking tot het beëindigen van de relatie. Zie voor meer informatie het onderwerp 'contract' in dit document.

4.3. Risicoanalyse

Een belangrijk onderdeel van het uitbestedingsproces is het maken van een risicoanalyse en het uitvoeren van een due diligence op de nieuwe dienstverlener. De AFM heeft in haar recente uitvraag omtrent uitbesteding een indicatie gegeven met betrekking tot de elementen die opgenomen kunnen worden in de due diligence procedure.

De due diligence procedure...

- vereist beoordeling van financiële risico's, waaronder de financiële situatie van de dienstverlener
- vereist beoordeling van risico's voor de (kwaliteit van de dienstverlening aan de) klant en voor de maatschappij
- vereist beoordeling van het risico van vendor lock-in
- vereist beoordeling van continuiteitsrisico's
- vereist beoordeling van concentratierisico's
- vereist beoordeling van conflicten als gevolg van cultuurverschillen tussen uw onderneming en de leverancier
- vereist beoordeling van informatiebeveiligingsrisico's
- vereist beoordeling van politieke risico's zoals risico's met betrekking tot de locatie van data
- vereist beoordeling van risico's door belangenconflicten
- maakt onderscheid tussen intragroepuitbesteding en reguliere uitbesteding
- stelt dat ten minste JZ, Risk, Compliance en de business bij de due dilligence betrokken is
- toetst of de dienstverlener ten minste aan alle wettelijke vereisten kan voldoen

- toetst of en in welke mate de dienstverlener aan de gestelde wensen en eisen van de onderneming kan voldoen

De belangrijkste risico's zijn door DNB in een 'risicoanalyse template uitbesteding' opgenomen. Beleggingsondernemingen kunnen deze template gebruiken en waar nodig aanvullen met andere risico's. Zie voor meer informatie: https://www.toezicht.dnb.nl/5/50-237322.jsp In Bijlage 2 van dit document is de template van DNB opgenomen en hebben wij tevens waar mogelijk een opmerking gemaakt over mitigerende maatregelen bij uitbesteding aan Blanco. En ook hier geldt: wij denken graag met u mee, maar u zult zelf kritisch een analyse moeten uitvoeren.

4.4. Contract

Op basis van richtsnoer 75 van de EBA richtsnoeren dient de uitbestedingsovereenkomst ten minst onderstaande onderwerpen te behelzen. Graag geven wij hieronder aan of de (standaard) overeenkomst met Blanco het onderwerp adresseert en zo ja, hoe.

EBA-richtsnoeren	Blanco
Een heldere beschrijving van de te verrichten uitbestede functie.	De overeenkomst (Delivery Agreement) met Blanco bevat een omschrijving van de geleverde software en/of service.
De aanvangsdatum en einddatum, indien van toepassing, van de overeenkomst en de opzeggingstermijnen voor de dienstverlener en de instelling of betalingsinstelling	De overeenkomst bevat altijd een aanvangs- en einddatum, inclusief opzeggingsclausule(s).
De wetgeving die op de overeenkomst van toepassing is	De toepasselijke wetgeving is altijd onderdeel van de overeenkomst.
De financiële verplichtingen van de partijen	De financiële verplichtingen zijn altijd onderdeel van de overeenkomst.
Of de onderuitbesteding van een kritieke of belangrijke functie, of materiële onderdelen daarvan, is toegestaan en zo ja, de in paragraaf 13.1 vermelde voorwaarden die voor de onderuitbesteding gelden	Onderuitbesteding is mogelijk onder de overeenkomst; een goed voorbeeld van onderuitbesteding bij Blanco is de cloudprovider (Maincubes en AWS). Daarnaast ontsluit Blanco via haar platform diensten van derden, zoals van ComplyAdvantage, de KvK en Mitek. Niet alle voorwaarden voor onderuitbesteding zijn concreet gemaakt in de overeenkomst, maar Blanco dient op basis van de overeenkomst de klant altijd te informeren indien na aanvang van de dienstverlening aan een nieuwe partij wordt onderuitbesteed. In dat geval kan er altijd aanvullende informatie aan Blanco worden gevraagd met betrekking tot de betreffende partij en indien de onderuitbesteding niet akkoord is, heeft de klant de mogelijkheid om een deel van de dienst niet of anders te gebruiken of om de overeenkomst op te zeggen. Blanco doet altijd een gedegen onderzoek naar de

	partijen aan wie werkzaamheden worden uitbesteed.
De locatie(s) (d.w.z. regio's of landen) waar de kritieke of belangrijke functie zal worden verricht en/of waar de relevante gegevens zullen worden bewaard en verwerkt, inclusief de mogelijke opslaglocatie, en de voorwaarden waaraan moet worden voldaan, met inbegrip van de vereiste om de instelling of betalingsinstelling in kennis te stellen als de dienstverlener voorstelt de locatie(s) te wijzigen	Blanco verwerkt gegevens in Nederland en België en gebruikt daarbij de diensten van Maincubes (Nederland) en van AWS (regio Frankfurt – Duitsland). Andere derde partijen en de locatie van gegevensverwerking zijn opgenomen in de Delivery Agreement. In de verwerkersovereenkomst zijn de technische en organisatorische maatregelen opgenomen die Blanco treft. Deze maatregelen en andere maatregelen zijn in scope van de ISAE3402. Op verzoek kan Blanco nadere informatie verschaffen over de informatiebeveiliging.
Waar relevant, bepalingen inzake de toegankelijkheid, beschikbaarheid, integriteit, privacy en veiligheid van de betrokken gegevens, als vermeld in paragraaf 13.2;	Zie hierboven. Informatiebeveiliging is een zeer belangrijk thema binnen Blanco en is onderdeel van de ISAE3402. Op verzoek kan Blanco nadere informatie verschaffen over de informatiebeveiliging.
Het recht van de instelling of betalingsinstelling om de prestaties van de dienstverlener doorlopend te bewaken;	Dit recht verkrijgt de klant op verschillende wijzen. In de eerste plaats wordt een servicelevel agreement overeengekomen. Daarnaast bevat de overeenkomst een right to audit en kan de klant de ISAE3402 rapportage inzien. Daarnaast kan de klant natuurlijk de prestaties op dagelijkse basis bij het gebruik toetsen en contact opnemen indien de dienstverlening niet voldoet.
De verplichtingen van de dienstverlener betreffende rapportage aan de instelling of betalingsinstelling, inclusief het melden door de dienstverlener van elke ontwikkeling die materiële gevolgen kan hebben voor het vermogen van de dienstverlener om de kritieke of belangrijke functie doeltreffend uit te voeren in lijn met de overeengekomen dienstverleningsniveaus en conform de toepasselijke wet- en regelgeving en, indien van toepassing, de verplichting om verslagen van de interne auditfunctie van de dienstverlener te overleggen	In de overeenkomst is opgenomen dat Blanco de klant informeert indien er veranderingen zijn die impact kunnen hebben op de dienstverlening.
Of de dienstverlener zich verplicht tegen bepaalde risico's dient te verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking	De verplichting tot verzekering is niet opgenomen in de overeenkomst, maar Blanco beschikt uiteraard over een beroepsaansprakelijkheidsverzekering. Op

	verzoek kan er inzage worden verkregen in de polis.
Bepalingen die ervoor zorgen dat toegang kan worden verkregen in de gegevens die het eigendom van de instelling of betalingsinstelling zijn, wanneer de dienstverlener insolvent is, zich in een afwikkelingsproces bevindt of zijn bedrijfsactiviteiten beëindigt	In de overeenkomst is opgenomen dat de data van de klant het eigendom blijft van de klant. De klant heeft een instructierecht met betrekking tot zijn data, zoals opgenomen in de verwerkersovereenkomst. In geval van een faillissement van Blanco is er contractueel een continuïteitsmaatregel overeengekomen, waarbij een stichting tijdelijk de dienstverlening van Blanco overneemt, zodat de beleggingsonderneming een andere leverancier kan selecteren of kan besluiten de diensten zelf uit te voeren. In de continuïteitsovereenkomst is tevens een instructierecht opgenomen.
De verplichting van de dienstverlener om met de bevoegde autoriteiten en afwikkelingsautoriteiten van de instelling of betalingsinstelling samen te werken, met inbegrip van andere personen die door hen zijn aangewezen	Deze verplichting is onderdeel van de overeenkomst.
Voor instellingen een duidelijke verwijzing naar de bevoegdheden van de nationale afwikkelingsautoriteit, vooral naar de artikelen 68 en 71 van Richtlijn 2014/59/EU (BRRD), en met name een beschrijving van de "materiële verplichtingen" van het contract in de zin van artikel 68 van die richtlijn	Deze bepaling is over het algemeen niet van toepassing.
Het onbeperkte recht van instellingen, betalingsinstellingen en bevoegde autoriteiten om de dienstverlener te inspecteren en te controleren, vooral als het gaat om de kritieke of belangrijke uitbestede functie, als vermeld in paragraaf 13.3	Deze verplichting is onderdeel van de overeenkomst.
Beëindigingsrechten, als vermeld in paragraaf 13.4	In de overeenkomst zijn afspraken gemaakt over beëindiging van de overeenkomst. Tevens is er een bepaling opgenomen met betrekking tot exit assistentie, waarbij Blanco aangeeft een overdracht aan een opvolgende dienstverlener te zullen faciliteren.

Indien u langere tijd geleden een overeenkomst heeft gesloten met Blanco of AIRS, zou het kunnen dat (mede door inwerkingtreding van nieuwe wetgeving of publicatie van aanvullende richtsnoeren) uw contract niet alle informatie bevat zoals hierboven aangegeven. U kunt in dat geval de gewenste informatie bij ons opvragen, of een nieuwe

overeenkomst met ons sluiten – uiteraard zonder wezenlijke inhoudelijke veranderingen ten aanzien van bijvoorbeeld de looptijd of de tarieven.

4.5. Meldingen toezichthouder

Beleggingsondernemingen dienen bij de AFM melding te doen van materiële activiteiten die de beleggingsonderneming heeft uitbesteed. Het gaat daarbij om activiteiten die betrekking hebben op het primaire proces van de onderneming. De melding moet worden gedaan voordat de activiteit wordt uitbesteed aan een dienstverlener. Zie voor meer informatie en het meldingsformulier: https://www.afm.nl/nl-nl/professionals/onderwerpen/uitbesteding-doorlopend-melden-bobi

Vrijwel alle informatie die u nodig heeft kunt u vinden in dit document en/of in de overeenkomst die u met Blanco sluit of heeft gesloten. Additionele informatie kan altijd worden opgevraagd.

4.6. Evaluatie van de uitbesteding

Gedurende de looptijd van de overeenkomst dient u regelmatig uw dienstverleners te evalueren. Daarbij gaat het onder andere om het evalueren van wijzigingen die zich bij de dienstverlener voordoen, zoals een belangrijke wijziging van de eigendomsverhoudingen, de strategie of de winstgevendheid. (Zoals hierboven al aangegeven is in de overeenkomst met Blanco al opgenomen dat Blanco u zal informeren over relevante wijzigingen in de onderneming en/of het product wanneer deze zich voordoen.)

Om de evaluatie van uw dienstverleners te structureren, verdient het aanbeveling om een evaluatieprocedure in te richten. De AFM heeft in haar recente uitvraag omtrent uitbesteding een indicatie gegeven met betrekking tot de elementen die opgenomen kunnen worden in de evaluatie procedure.

De kwaliteitsbeoordeling...

- stelt dat kwaliteitseisen aan uitbestede diensten meetbaar gedefinieerd zijn
- stelt dat kwaliteitseisen aan uitbestede diensten overeengekomen zijn en schriftelijk zijn vastgelegd in servicelevel agreements
- stelt dat voor elke uitbesteding overeengekomen moet zijn welke stappen/procedures en consequenties volgen op het niet halen van overeengekomen kwaliteitsniveaus
- vereist dat de dienstverlener de onderneming inzicht geeft in de werkelijk behaalde servicelevels binnen de overeengekomen frequentie
- vereist dat de onderneming het recht heeft en de mogelijkheid krijgt om onderzoek te doen bij de dienstverlener naar de kwaliteit van de dienstverlening
- verplicht de dienstverlener om incidenten in relatie tot de dienstverlening te rapporteren in een vooraf overeengekomen frequentie
- schrijft voor welke stappen/procedures de onderneming volgt wanneer de dienstverlener niet voldoet aan de contractvoorwaarden
- schrijft voor dat continuiteitsrisico's periodiek worden geïdentificeerd en geëvalueerd
- schrijft voor dat continuiteitswaarborgen van leveranciers ten minste jaarlijks worden beoordeeld
- schrijft voor dat de opvolging van wensen en eisen ten aanzien van de dienstverlening periodiek worden beoordeeld

- schrijft voor dat voor elke uitbesteding periodiek assurance over het stelsel van interne beheersing wordt geleverd
- schrijft voor dat informatiebeveiliging onderdeel is van de periodieke assurance die de dienstverlener over de geboden dienstverlening levert

Met betrekking tot de uitbesteding aan Blanco hebben wij hierboven al aangegeven dat Blanco de evaluatie van de dienstverlening op verschillende manier probeert te vergemakkelijken. In de eerste plaats wordt een servicelevel agreement overeengekomen, waarover ook gerapporteerd wordt. Ook bevat de overeenkomst een right to audit en kan de klant de ISAE3402 rapportage inzien. Daarnaast kan de klant natuurlijk de prestaties op dagelijkse basis bij het gebruik toetsen en contact opnemen indien de dienstverlening niet voldoet.

4.7. Register

Beleggingsondernemingen dienen een register bij te houden met informatie over alle uitbestedingen. Op grond van de EBA richtsnoeren (richtsnoer 54) zou dit register de volgende informatie moeten bevatten:

a) een referentienummer voor elke uitbestedingsregeling;
b) de aanvangsdatum en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, de einddatum en/of opzeggingstermijnen voor de dienstverlener en voor de instelling of betalingsinstelling;
c) een korte beschrijving van de uitbestede functie, inclusief de gegevens die worden uitbesteed en of persoonsgegevens al dan niet zijn overgedragen (bijv. door ja of nee in een afzonderlijk gegevensveld te vermelden), of dat de verwerking daarvan aan een dienstverlener wordt uitbesteed;
d) een door de onderneming toegewezen categorie die de aard van de functie als beschreven onder c) weerspiegelt (bijv. informatietechnologie (IT), controlefunctie), waardoor de inventarisatie van verschillende soorten regelingen gemakkelijker wordt;
e) de naam van de dienstverlener, het handelsregisternummer, de identificatiecode voor de rechtspersoon (indien beschikbaar), het geregistreerde adres en andere relevante contactgegevens, en de naam van de moederonderneming (indien aanwezig);
f) het land of de landen waar de dienst wordt verricht, inclusief de locatie (d.w.z. land of regio) van de gegevens;
g) of de uitbestede functie al dan niet (ja/nee) als kritiek of belangrijk wordt beschouwd, plus, indien van toepassing, een korte samenvatting van de redenen waarom de uitbestede functie als kritiek of belangrijk wordt beschouwd;
h) in het geval van uitbesteding aan een aanbieder van clouddiensten, de modellen voor de clouddiensten en de uitrol van de cloud, d.w.z. publiek/privaat/hybride/gemeenschappelijk, en de specifieke aard van de te bewaren gegevens en de locaties (d.w.z. landen of regio's) waar die gegevens worden opgeslagen;
i) de datum waarop het kritieke karakter of het belang van de uitbestede functie voor het laatst zijn beoordeeld.

Met het oog op de uitbesteding van kritieke of belangrijke functies bevat het register ten minste de volgende aanvullende informatie:

a) de instellingen, betalingsinstellingen en andere ondernemingen binnen de prudentiële consolidatie of het institutionele protectiestelsel, indien van toepassing, die van de uitbesteding gebruikmaken;
b) of de dienstverlener of onderdienstverlener deel uitmaakt van de groep of bij het institutionele protectiestelsel is aangesloten of het eigendom is van instellingen of betalingsinstellingen binnen de groep of het eigendom is van de leden van een institutioneel protectiestelsel;
c) de datum waarop voor het laatst een risicobeoordeling heeft plaatsgevonden, en een korte samenvatting van de belangrijkste resultaten;
d) de persoon of het besluitvormingsorgaan (bijv. het leidinggevend orgaan) in de instelling of de betalingsinstelling die de uitbestedingsregeling heeft goedgekeurd;
e) de wetgeving die op de uitbestedingsregeling van toepassing is;
f) de data van de meest recente en volgende geplande audits, indien van toepassing.
g) indien van toepassing, de namen van onderaannemers waaraan materiële onderdelen van een kritieke of belangrijke functie zijn onderuitbesteed, inclusief het land waar de onderaannemers zijn geregistreerd, waar de dienst zal worden verricht en, indien van toepassing, de locatie (d.w.z. land of regio) waar de gegevens zullen worden opgeslagen;
h) de uitkomsten van de beoordeling van de vervangbaarheid van de dienstverlener (als gemakkelijk, moeilijk of onmogelijk), de mogelijkheid om een kritieke of belangrijke functie opnieuw in de instelling of de betalingsinstelling te integreren of het effect van het beëindigen van de kritieke of belangrijke functie;
i) alternatieve dienstverleners in overeenstemming met h);
j) of de uitbestede kritieke of belangrijke functie tijdgevoelige bedrijfsactiviteiten ondersteunt;
k) de geraamde jaarlijkse begrotingskosten.

Bijlage 1 – EBA Richtsnoeren inzake uitbesteding

	Richtsnoeren	Implementatie bij beleggingsonderneming (*Input Blanco bij uitvoeren analyse)*
	Titel I – Evenredigheid: toepassing binnen groepen en institutionele protectiestelsels	
	1. Evenredigheid	
18.	Instellingen, betalingsinstellingen en bevoegde autoriteiten houden bij de naleving van of het toezicht op de naleving van deze richtsnoeren rekening met het evenredigheidsbeginsel. Het evenredigheidsbeginsel heeft tot doel ervoor te zorgen dat governanceregelingen, inclusief de regelingen met betrekking tot uitbesteding, in overeenstemming zijn met het individuele risicoprofiel, de aard en het bedrijfsmodel van de instelling of betalingsinstelling, en de omvang en complexiteit van haar activiteiten, zodat de doelstellingen van de regelgevende vereisten doeltreffend worden verwezenlijkt.	*Houd rekening met het evenredigheidsbeginsel*
19.	Instellingen en betalingsinstellingen houden bij het toepassen van de voorschriften van deze richtsnoeren rekening met de complexiteit van de uitbestede functies, de risico's die uit de uitbestedingsregelingen voortvloeien, het kritieke karakter of het belang van de uitbestede functie en de mogelijke gevolgen van de uitbesteding voor de continuïteit van hun activiteiten	*Houd rekening met het evenredigheidsbeginsel*
20.	Bij het toepassen van het evenredigheidsbeginsel nemen instellingen, betalingsinstellingen en bevoegde autoriteiten de criteria in acht die worden genoemd in titel I van de EBA- richtsnoeren inzake interne governance in overeenstemming met artikel 74, lid 2, van Richtlijn 2013/36/EU.	*Houd rekening met het evenredigheidsbeginsel*
	2. Uitbesteding door groepen en instellingen die zijn aangesloten bij een institutioneel protectiestelsel	
21.	In overeenstemming met artikel 109, lid 2, van Richtlijn 2013/36/EU gelden deze richtsnoeren ook op gesubconsolideerde en geconsolideerde basis, met inachtneming van het bereik van de prudentiële consolidatie. Met het oog hierop zorgen EU-moederondernemingen of de moederonderneming in een lidstaat ervoor dat regelingen, processen en mechanismen voor interne governance in hun dochterondernemingen, inclusief betalingsinstellingen, consistent, goed geïntegreerd en adequaat zijn, zodat deze richtsnoeren op alle relevante niveaus doeltreffend worden toegepast.	*Deze paragraaf is veelal niet van toepassing*

22.	Instellingen en betalingsinstellingen overeenkomstig punt 21, en instellingen die, als aangeslotenen bij een institutioneel protectiestelsel, van centraal getroffen governanceregelingen gebruikmaken, voldoen aan het volgende: a. Wanneer die instellingen of betalingsinstellingen een uitbestedingsregeling met dienstverleners binnen de groep of het institutionele protectiestelsel hebben, blijft het leidinggevend orgaan van die instellingen of betalingsinstellingen, ook wat deze uitbestedingsregeling betreft, volledig verantwoordelijk voor de naleving van alle regelgevingsvereisten en de doeltreffende toepassing van deze richtsnoeren. b. Wanneer die instellingen of betalingsinstellingen de operationele taken van interne controlefuncties aan een dienstverlener binnen de groep of het institutionele protectiestelsel uitbesteden om uitbestedingsregelingen te bewaken en te controleren, zorgen de instellingen ervoor dat, ook wat deze uitbestedingsregelingen betreft, die operationele taken doeltreffend worden uitgevoerd, onder meer via het ontvangen van passende verslagen	*Deze paragraaf is veelal niet van toepassing*
23	In aanvulling op punt 22 houden instellingen en betalingsinstellingen binnen een groep waarvoor geen vrijstellingen zijn verleend op grond van artikel 109 van Richtlijn 2013/36/EU en artikel 7 van Verordening (EU) nr. 575/2013, instellingen die een centraal orgaan zijn of die blijvend zijn aangesloten bij een centraal orgaan waarvoor geen vrijstellingen zijn verleend op grond van artikel 21 van Richtlijn 2013/36/EU, of instellingen die zijn aangesloten bij een institutioneel protectiestelsel, rekening met het volgende: a. Wanneer de operationele bewaking van de uitbesteding wordt gecentraliseerd (bijv. als onderdeel van een raamovereenkomst voor de bewaking van uitbestedingsregelingen), zorgen instellingen en betalingsinstellingen ervoor dat, in elk geval voor uitbestede kritieke of belangrijke functies, zowel de onafhankelijke bewaking van de dienstverlener als een passend toezicht door elke instelling of betalingsinstelling mogelijk zijn, onder meer door - ten minste jaarlijks en op verzoek van de gecentraliseerde bewakingsfunctie - verslagen te ontvangen die in elk geval een samenvatting van de risicobeoordeling en de prestatiebewaking omvatten. Daarnaast ontvangen instellingen en betalingsinstellingen van de gecentraliseerde bewakingsfunctie een samenvatting van de relevante auditverslagen over de uitbesteding van kritieke of belangrijke functies en, op verzoek, het complete auditverslag. b. Instellingen en betalingsinstellingen zorgen ervoor dat hun leidinggevend orgaan naar behoren op de hoogte wordt gebracht van de relevante geplande wijzigingen wat betreft de dienstverleners die centraal worden bewaakt, en de mogelijke gevolgen van deze wijzigingen voor de verrichte kritieke of belangrijke functies, inclusief een samenvatting van de risicoanalyse, waaronder juridische risico's, naleving van de regelgevingsvereisten en het effect op het niveau van de dienstverlening, zodat het leidinggevend orgaan de gevolgen van deze wijzigingen kan beoordelen;. c. Wanneer die instellingen en betalingsinstellingen binnen de groep, instellingen die bij een centraal orgaan zijn aangesloten, of instellingen die tot een institutioneel protectiestelsel behoren, steunen op een centrale voorafgaande beoordeling van uitbestedingsregelingen, als bedoeld in hoofdstuk 12, ontvangt elke instelling en betalingsinstelling een samenvatting van de beoordeling en houdt zij rekening met de specifieke structuur en risico's ervan binnen het besluitvormingsproces. d. Wanneer het register van alle bestaande uitbestedingsregelingen, als bedoeld in hoofdstuk 11, centraal wordt opgesteld en bijgehouden binnen een groep of institutioneel protectiestelsel, zijn bevoegde autoriteiten, alle instellingen en betalingsinstellingen in staat zonder onnodig uitstel hun individuele register te verkrijgen. Dit register omvat alle uitbestedingsregelingen, inclusief uitbestedingsregelingen met dienstverleners binnen die groep of dat institutionele protectiestelsel. e. Wanneer die instellingen en betalingsinstellingen steunen op een exitplan voor een kritieke of belangrijke functie dat op groepsniveau is opgesteld, binnen het institutionele protectiestelsel of door	*Deze paragraaf is veelal niet van toepassing*

	het centraal orgaan, ontvangen alle instellingen en betalingsinstellingen een samenvatting van het plan en vergewissen zij zich zich ervan dat het plan doeltreffend kan worden uitgevoerd.	
24.	Wanneer vrijstellingen zijn verleend op grond van artikel 21 of artikel 109, lid 1, van Richtlijn 2013/36/EU in samenhang met artikel 7 van Verordening (EU) nr. 575/2013, worden de bepalingen van deze richtsnoeren door de moederonderneming in een lidstaat toegepast voor zichzelf en haar dochterondernemingen of door het centraal orgaan en de daarbij aangesloten instellingen als geheel.	*Deze paragraaf is veelal niet van toepassing*
25.	Instellingen en betalingsinstellingen die dochterondernemingen van een EU- moederonderneming of een moederonderneming in een lidstaat vormen waaraan geen vrijstellingen zijn verleend op grond van artikel 21 of artikel 109, lid 1, van Richtlijn 2013/36/EU in samenhang met artikel 7 van Verordening (EU) nr. 575/2013, zorgen ervoor dat zij elk afzonderlijk aan deze richtsnoeren voldoen.	*Deze paragraaf is veelal niet van toepassing*
	Titel II – Beoordeling van uitbestedingsregelingen	
	3. Uitbesteding	
26.	Instellingen en betalingsinstellingen bepalen of een regeling met een derde onder de definitie van uitbesteding valt. Bij deze beoordeling wordt mee gewogen in hoeverre de functie (of een onderdeel daarvan) die (dat) aan een dienstverlener wordt uitbesteed, periodiek of doorlopend door de dienstverlener wordt verricht en of deze functie (of een deel daarvan) gewoonlijk tot de functies behoort die realistisch gezien door instellingen of betalingsinstellingen zouden of zouden kunnen worden verricht, zelfs als de instelling of betalingsinstelling deze functie in het verleden niet zelf heeft verricht.	*Zie tevens hoofdstuk 2 van de Blanco-paper*
27.	Wanneer een regeling met een dienstverlener meerdere functies omvat, kijken instellingen en betalingsinstellingen bij hun beoordeling naar alle aspecten van de regeling, bijv. als de verleende dienst het aanbieden van hardware voor gegevensopslag en de back-up van gegevens omvat, worden beide aspecten gezamenlijk in ogenschouw genomen.	*Voer voorafgaand aan een uitbesteding altijd een risico-analyse uit, waarbij alle relevante aspecten van de totale uitbesteding in samenhang worden bekeken.*
28.	Als algemeen beginsel beschouwen instellingen en betalingsinstellingen het volgende niet als uitbesteding: a. een functie die volgens de wet door een dienstverlener moet worden uitgevoerd, bijv. een wettelijke audit; b. marktinformatiediensten (bijv. verstrekken van gegevens door Bloomberg, Moody's, Standard & Poor's, Fitch); c. mondiale netwerkinfrastructuren (bijv. Visa, MasterCard); d. clearing- en afwikkelingsregelingen tussen clearinginstituten, centrale tegenpartijen en afwikkelingsinstellingen en de leden daarvan; e. mondiale infrastructuren voor het financiële berichtenverkeer die onder toezicht van de desbetreffende autoriteiten staan; f. diensten van correspondentbanken; en g. de aankoop van diensten die anders niet door de instelling of betalingsinstelling zouden worden verricht (bijv. advies van een architect, verstrekken van juridisch advies en vertegenwoordiging bij de rechtbank en bestuursorganen, schoonmaken, tuinieren en onderhoud op het terrein van de instelling of betalingsinstelling, medische diensten, onderhoud van bedrijfsauto's, catering, service in verband met automaten, administratieve dienstverlening, diensten in verband met reizen of de postkamer, receptionisten, secretaresses en telefonisten), goederen (bijv. plastic kaarten, kaartlezers, kantoorbenodigdheden, personal computers, meubilair) of nutsvoorzieningen (bijv. elektriciteit, gas, water, telefoonlijn).	*Ter informatie/geen opmerkingen*

	4 Kritieke of belangrijke functies	
29.	In de volgende situaties beschouwen instellingen en betalingsinstellingen een functie altijd als kritiek of belangrijk: a. wanneer een gebrekkige of tekortschietende uitvoering ervan materiële nadelige gevolgen zou hebben voor: i. het voortdurend voldoen door deze instellingen aan de vergunningsvoorwaarden of andere verplichtingen waaraan zij uit hoofde van Richtlijn 2013/36/EU, Verordening (EU) nr. 575/2013, Richtlijn 2014/65/EU, Richtlijn (EU) 2015/2366 en Richtlijn 2009/110/EG zijn onderworpen, en van hun regelgevingsverplichtingen; ii. hun financiële resultaten; of iii. de soliditeit of continuïteit van hun bank- en betalingsdiensten en -activiteiten; b. wanneer operationele taken van interne controlefuncties worden uitbesteed, tenzij uit de beoordeling blijkt dat het geen nadelige gevolgen voor de doeltreffendheid van de interne controlefunctie zou hebben als de uitbestede functie niet of op onjuiste wijze zou worden verricht; c. wanneer zij van plan zijn functies van bankactiviteiten of betalingsdiensten op zo'n schaal uit te besteden dat daarvoor toestemming van een bevoegde autoriteit nodig is, als bedoeld in paragraaf 12.1.	*Ter informatie/geen opmerkingen*
30.	In het geval van instellingen wordt bijzondere aandacht geschonken aan de beoordeling van het kritieke karakter of het belang van functies, als de uitbesteding betrekking heeft op functies die verband houden met kernbedrijfsonderdelen en kritieke functies zoals gedefinieerd in artikel 2, lid 1, punten 35 en 36, van Richtlijn 2014/5918 en vastgesteld door instellingen op grond van de criteria van de artikelen 6 en 7 van Gedelegeerde Verordening (EU) 2016/778 van de Commissie. Functies die nodig zijn om activiteiten van kernbedrijfsonderdelen of kritieke functies uit te voeren, worden in het kader van deze richtsnoeren als kritieke of belangrijke functies beschouwd, tenzij uit de beoordeling van de instelling blijkt dat het geen nadelige gevolgen voor de operationele continuïteit van het kernbedrijfsonderdeel of de kritieke functie zou hebben als de uitbestede functie niet of op onjuiste wijze zou worden verricht.	*Ter informatie/geen opmerkingen*
31.	Om te beoordelen of een uitbestedingsregeling betrekking heeft op een functie die kritiek of belangrijk is, houden instellingen en betalingsinstellingen niet alleen rekening met de uitkomsten van de risicobeoordeling als beschreven in paragraaf 12.2, maar ten minste ook met de volgende factoren: a. of de uitbestedingsregeling rechtstreeks verband houdt met het verrichten van bankactiviteiten of het verlenen van betalingsdiensten waarvoor zij een vergunning hebben; b. de mogelijke gevolgen van een verstoring van de uitbestede functie of van het feit dat de dienstverlener de dienst niet voortdurend op de overeengekomen niveaus van dienstverlening verricht, voor hun: i. financiële veerkracht en levensvatbaarheid op de korte en lange termijn, inclusief indien van toepassing, hun activa, kapitaal, kosten, financiering, liquiditeit, winsten en verliezen; ii. bedrijfscontinuïteit en operationele veerkracht; iii. operationele risico, inclusief gedrag, informatie- en communicatietechnologie (ICT) en juridische risico's; iv. reputatierisico's; v. indien van toepassing, herstel- en afwikkelingsplanning, afwikkelbaarheid en operationele continuïteit bij vroegtijdige interventie, herstel of afwikkeling; c. de mogelijke gevolgen van de uitbestedingsregeling voor hun vermogen om: i. alle risico's te identificeren, te bewaken en te beheren; ii. aan alle wettelijke en regelgevingsvereisten te voldoen; iii. passende audits op de uitbestede functie te verrichten;	*Ter informatie/geen opmerkingen*

	d. de mogelijke gevolgen voor de diensten die zij aan hun cliënten verlenen; e. alle uitbestedingsregelingen, de geaggregeerde blootstelling van de instelling of betalingsinstelling aan dezelfde dienstverlener en de mogelijke cumulatieve gevolgen van uitbestedingsregelingen op hetzelfde werkterrein; f. de omvang en complexiteit van elk betrokken werkterrein; g. de mogelijkheid om de voorgestelde uitbestedingsregeling op te schalen zonder de onderliggende overeenkomst te vervangen of te herzien; h. de mate waarin het mogelijk is om de voorgestelde uitbestedingsregeling indien nodig of wenselijk, zowel contractueel als in de praktijk, aan een andere dienstverlener over te dragen, inclusief de geraamde risico's, belemmeringen voor de bedrijfscontinuïteit, kosten en het tijdschema daarvoor ("vervangbaarheid"); i. de mate waarin het mogelijk is om de uitbestede functie opnieuw in de instelling of betalingsinstelling te integreren, als dat nodig of wenselijk is; j. de bescherming van gegevens en de mogelijke gevolgen van een schending van de vertrouwelijkheid of waarborging van de beschikbaarheid en integriteit van gegevens voor de instelling of betalingsinstelling en haar cliënten, inclusief maar niet beperkt tot de naleving van Verordening (EU) 2016/67921.	
	Titel III – Kader voor governance	
	5. Solide governanceregelingen en risico's die samenhangen met derden	
32.	Instellingen beschikken als onderdeel van het algehele kader voor interne controle, met inbegrip van interne controlemechanismen, over een holistisch, instellingsbreed kader voor risicobeheer dat zich uitstrekt over alle bedrijfsonderdelen en interne eenheden. Op grond van dat kader identificeren en beheren instellingen en betalingsinstellingen al hun risico's, inclusief risico's die worden veroorzaakt door regelingen met derden. Het kader voor risicobeheer stelt instellingen en betalingsinstellingen tevens in staat goed geïnformeerde besluiten te nemen over het aangaan van risico's en zorgt ervoor dat maatregelen op het gebied van risicobeheer op de juiste wijze worden uitgevoerd, ook met betrekking tot cyberrisico's	*Zorg voor een instelling breed kader voor risicobeheer, dat zich uitstrekt over alle bedrijfsonderdelen. Voorbeelden hiervan zijn een risk management proces dat periodiek wordt doorlopen, het uitvoeren van periodieke integriteit risico-analyses en het doorlopend monitoren en/of controleren van processen die zowel intern als door een uitbestedingspartner worden uitgevoerd.*
33.	Instellingen en betalingsinstellingen identificeren, beoordelen, bewaken en beheren, met inachtneming van het evenredigheidsbeginsel in lijn met hoofdstuk 1, alle risico's die voortvloeien uit regelingen met derden waaraan zij zijn of kunnen worden blootgesteld, ongeacht of die regelingen uitbestedingsregelingen vormen. De risico's, met name de operationele risico's, van alle regelingen met derden, inclusief de risico's als bedoeld in de punten 26 en 28, worden in overeenstemming met paragraaf 12.2 beoordeeld.	*De uitbestede diensten dienen onderdeel te zijn van het interne risicobeheer.*
34.	Instellingen en betalingsinstellingen voldoen aan alle voorschriften van Verordening (EU) 2016/679, ook wat betreft hun regelingen met derden en uitbestedingsregelingen.	*Ter informatie/geen opmerkingen*
	6. Solide governanceregelingen en uitbesteding	
35.	Uitbesteding van functies kan er niet toe leiden dat de verantwoordelijkheden van het leidinggevend orgaan worden gedelegeerd. Instellingen en betalingsinstellingen blijven volledig verantwoordelijk voor en rekenschap afleggen van de naleving van al hun regelgevingsverplichtingen, inclusief het vermogen om toezicht te houden op de uitbesteding van kritieke of belangrijke functies.	*Ter informatie/geen opmerkingen*

36.	Het leidinggevend orgaan is te allen tijde volledig verantwoordelijk voor en legt rekenschap af van in elk geval het volgende: a. ervoor zorgen dat de instelling of betalingsinstelling voortdurend voldoet aan de voorwaarden om haar vergunning te behouden, inclusief voorwaarden die de bevoegde autoriteit heeft opgelegd; b. de interne organisatie van de instelling of de betalingsinstelling; c. de identificatie, de beoordeling en het beheer van belangenconflicten; d. het vaststellen van de strategieën en het beleid van de instelling of betalingsinstelling (bijv. het bedrijfsmodel, de risicobereidheid, het kader voor risicobeheer); e. toezicht uitoefenen op het dagelijks beheer van de instelling of betalingsinstelling, inclusief het beheer van alle risico's die met uitbesteding verband houden; en f. de toezichthoudende rol van het leidinggevend orgaan, inclusief het toezicht op en de bewaking van de besluitvorming door het management.	*Ter informatie/geen opmerkingen*
37.	Uitbesteding mag er niet toe leiden dat lagere geschiktheidseisen worden gesteld aan de leden van het leidinggevend orgaan van een instelling, de bestuurders en de personen die verantwoordelijk zijn voor het beheer van de betalingsinstelling, en aan medewerkers met een sleutelfunctie. Instellingen en betalingsinstellingen beschikken over adequate vakbekwaamheid en over voldoende en goed opgeleid personeel zodat zij de uitbestedingsregelingen op passende wijze kunnen beheren en daarop toezicht kunnen houden.	*Ter informatie/geen opmerkingen*
38.	Instellingen en betalingsinstellingen: a. kennen de verantwoordelijkheden voor de documentatie, het beheer en de controle op uitbestedingsregelingen duidelijk toe; b. wijzen voldoende middelen toe om ervoor te zorgen dat alle wettelijke en regelgevingsvereisten worden nageleefd, inclusief deze richtsnoeren en de documentatie van en de bewaking van alle uitbestedingsregelingen; c. stellen een uitbestedingsfunctie in of wijzen een hoger personeelslid aan dat rechtstreeks verantwoording aan het leidinggevend orgaan moet afleggen (bijv. een sleutelfunctiehouder binnen een controlefunctie) en verantwoordelijk is voor het beheer van en het toezicht op de risico's van uitbestedingsregelingen als onderdeel van het interne controlekader van de instelling en voor het toezicht op de documentatie van uitbestedingsregelingen, dit alles met inachtneming van hoofdstuk 1 van deze richtsnoeren. Kleine en minder complexe instellingen of betalingsinstellingen zorgen ten minste voor een duidelijke verdeling van taken en verantwoordelijkheden voor het beheer van en de controle op uitbestedingsregelingen en kunnen de uitbestedingsfunctie aan een lid van het leidinggevend orgaan van de instelling of de betalingsinstelling toewijzen.	*Ter informatie/geen opmerkingen*
39.	Instellingen en betalingsinstellingen blijven te allen tijde voldoende inhoud bewaren en worden geen “lege hulzen” of “brievenbusmaatschappijen”. Hiertoe: a. voldoen zij te allen tijde aan de voorwaarden van hun vergunning, hetgeen ook inhoudt dat het leidinggevend orgaan doeltreffend zijn verantwoordelijkheden uitoefent zoals beschreven in punt 36 van deze richtsnoeren; b. houden zij een helder en transparant organisatiekader en een heldere en transparante structuur in stand die hen in staat stelt aan de wettelijke en regelgevingsvereisten te voldoen; c. oefenen zij passend toezicht uit en zijn zij in staat de risico's te beheren die het gevolg zijn van de uitbesteding van kritieke of belangrijke functies, wanneer de operationele taken van interne controlefuncties worden uitbesteed (bijv. in het geval van uitbesteding binnen de groep of uitbesteding binnen institutionele protectiestelsels); en d. hebben zij voldoende middelen en capaciteiten om a) tot en met c) na te leven.	*Ter informatie/geen opmerkingen*

40.	Bij het uitbesteden zorgen instellingen en betalingsinstellingen er in elk geval voor dat: a. zij besluiten kunnen nemen en uitvoeren die verband houden met hun bedrijfsactiviteiten en kritieke of belangrijke functies, inclusief de activiteiten en functies die zijn uitbesteed; b. zij op ordelijke wijze hun bedrijfsvoering en hun bank- en betalingsdiensten blijven verrichten; c. de risico's met betrekking tot de bestaande en geplande uitbestedingsregelingen adequaat worden geïdentificeerd, beoordeeld, beheerd en beperkt, inclusief risico's die verband houden met ICT en financiële technologie (FinTech); d. er passende regelingen bestaan voor de vertrouwelijkheid van gegevens en andere informatie; e. een adequate stroom van relevante informatie met dienstverleners in stand wordt gehouden; f. zij wat betreft de uitbesteding van kritieke of belangrijke functies ten minste een van de volgende handelingen kunnen verrichten, en wel binnen een passende termijn: i. de functie aan alternatieve dienstverleners overdragen; ii. de functie opnieuw integreren; of iii. de bedrijfsactiviteiten die van de functie afhankelijk zijn, staken. g. wanneer persoonsgegevens worden verwerkt door dienstverleners in de EU en/of derde landen, worden passende maatregelen getroffen en worden de gegevens verwerkt in overeenstemming met Verordening (EU) 2016/679.	*Ter informatie/geen opmerkingen*
	7. Uitbestedingsbeleid	
41.	Het leidinggevend orgaan van een instelling of betalingsinstelling die uitbestedingsregelingen heeft of van plan is zulke regelingen aan te gaan, keurt een schriftelijk uitbestedingsbeleid goed, herziet het regelmatig en werkt het bij, en zorgt, indien van toepassing, voor de tenuitvoerlegging daarvan op een individuele, gesubconsolideerde en geconsolideerde basis. Voor instellingen dient het uitbestedingsbeleid in overeenstemming te zijn met hoofdstuk 8 van de EBA-richtsnoeren inzake interne governance, in het bijzonder met inachtneming van de voorschriften in hoofdstuk 18 (Nieuwe producten en ingrijpende wijzigingen) van die richtsnoeren. Betalingsinstellingen kunnen hun beleid eveneens op de hoofdstukken 8 en 18 van de EBA-richtsnoeren inzake interne governance afstemmen.	*Zie tevens paragraaf 4.1 van de Blanco-paper*
42.	Het beleid omvat de belangrijkste fasen van de levenscyclus van uitbestedingsregelingen, met een omschrijving van de beginselen, verantwoordelijkheden en processen in relatie tot de uitbesteding. Het beleid behelst met name ten minste het volgende: a. de verantwoordelijkheden van het leidinggevend orgaan overeenkomstig punt 36, inclusief de betrokkenheid ervan, waar van toepassing, bij de besluitvorming over het uitbesteden van kritieke of belangrijke functies; b. de betrokkenheid van bedrijfsonderdelen, interne controlefuncties en andere personen ten aanzien van uitbestedingsregelingen; c. de planning van uitbestedingsregelingen, waaronder: i. de omschrijving van bedrijfsvoorschriften voor uitbestedingsregelingen; ii. de criteria, waaronder die welke worden genoemd in hoofdstuk 4, en processen voor het bepalen van kritieke of belangrijke functies; iii. de identificatie, beoordeling en het beheer van risico's in overeenstemming met paragraaf 12.2; iv. controles op de naleving van het zorgvuldigheidsbeginsel ("due diligence") bij mogelijke toekomstige dienstverleners, inclusief de maatregelen die op grond van paragraaf 12.3 zijn vereist; v. procedures voor de identificatie, de beoordeling, het beheer en de beperking van mogelijke belangenconflicten, in overeenstemming met hoofdstuk 8;	*Zie tevens paragraaf 4.1 van de Blanco-paper*

	vi. planning van de bedrijfscontinuïteit, in overeenstemming met hoofdstuk 9; vii. Wijze van goedkeuring van nieuwe uitbestedingsregelingen; d. de uitvoering, de bewaking en het beheer van uitbestedingsregelingen, inclusief: i. de continue beoordeling van de prestaties van de dienstverlener in overeenstemming met hoofdstuk 14; ii. de procedures voor de kennisgeving van en de reacties op veranderingen in een uitbestedingsregeling of dienstverlener (bijv. in zijn financiële positie, organisatie- of eigendomsstructuren, onderuitbesteding); iii. de onafhankelijke toetsing van en controle op de naleving van de wettelijke en regelgevingsvereisten en dito beleid; iv. de verlengingsprocedures; e. de documentatie en het bewaren van gegevens, met inachtneming van de voorschriften in hoofdstuk 11; f. de exitstrategieën en de beëindigingsprocedures, inclusief een voorschrift voor een gedocumenteerd exitplan voor elke uit te besteden kritieke of belangrijke functie, wanneer een dergelijke exit mogelijk wordt geacht, rekening houdend met mogelijke dienstonderbrekingen of de onverwachte beëindiging van een uitbestedingsregeling.	
43.	In het uitbestedingsbeleid wordt een onderscheid gemaakt tussen: a. uitbesteding van kritieke of belangrijke functies en andere uitbestedingsregelingen; b. uitbesteding aan dienstverleners die daarvoor van een bevoegde autoriteit een vergunning hebben gekregen en dienstverleners waarvoor dat niet geldt; c. uitbestedingsregelingen binnen de groep, uitbestedingsregelingen binnen hetzelfde institutionele protectiestelsel (inclusief entiteiten die individueel of collectief het eigendom zijn van instellingen binnen het institutionele protectiestelsel) en uitbesteding aan entiteiten buiten de groep; en d. uitbesteding aan dienstverleners in een lidstaat of derde land.	*Zie tevens paragraaf 4.1 van de Blanco-paper*
44.	Instellingen en betalingsinstellingen zien erop toe dat de vaststelling van de volgende mogelijke effecten van kritieke of belangrijke uitbestedingsregelingen onderdeel van het beleid vormen en dat daarmee tijdens de besluitvorming rekening wordt gehouden: a. het risicoprofiel van de instelling; b. het vermogen om toezicht op de dienstverlener te houden en de risico's te beheren; c. de maatregelen met het oog op de bedrijfscontinuïteit; en d. de uitoefening van hun bedrijfsactiviteiten.	*Zie tevens paragraaf 4.1 van de Blanco-paper*
	8. Belangenconflicten	
45.	Instellingen en betalingsinstellingen identificeren, beoordelen en beheren belangenconflicten met betrekking tot hun uitbestedingsregelingen; de instellingen doen dat in overeenstemming met titel IV, hoofdstuk 11, van de EBA-richtsnoeren inzake interne governance	*Als beleggingsonderneming dient u te beschikken over een belangenconflictenbeleid, waarin ook belangenconflicten bij uitbesteding worden meegenomen.*
46.	Wanneer door uitbesteding materiële belangenconflicten ontstaan, ook tussen entiteiten binnen dezelfde groep of hetzelfde institutionele protectiestelsel, moeten instellingen en betalingsinstellingen passende maatregelen nemen om deze belangenconflicten te beheren.	*Ter informatie/geen opmerkingen*

47.	Wanneer functies worden verricht door een dienstverlener die deel uitmaakt van een groep of van een institutioneel protectiestelsel of die het eigendom is van een instelling, betalingsinstelling, groep of instellingen die bij een institutioneel protectiestelsel zijn aangesloten, worden de voorwaarden, inclusief financiële voorwaarden, voor de uitbestede dienst marktconform vastgesteld. Bij de beprijzing van diensten kunnen synergiën die het gevolg zijn van het verlenen van dezelfde of soortgelijke diensten aan meerdere instellingen binnen een groep of een institutioneel protectiestelsel mee in aanmerking worden genomen, zolang de dienstverlener op zelfstandige basis levensvatbaar blijft; binnen een groep dient dit los te staan van het falen van een andere entiteit van de groep.	*Ter informatie/geen opmerkingen*
	9. Bedrijfscontinuïteitsplannen	
48.	Instellingen en betalingsinstellingen hebben passende bedrijfscontinuïteitsplannen met betrekking tot uitbestede kritieke of belangrijke functies, onderhouden deze en testen ze periodiek; instellingen doen dat in lijn met de voorschriften van artikel 85, lid 2, van Richtlijn 2013/36/EU en titel VI van de EBA-richtsnoeren inzake interne governance28. Instellingen en betalingsinstellingen binnen een groep of institutioneel protectiestelsel kunnen wat betreft hun uitbestede functies steunen op centraal opgestelde bedrijfscontinuïteitsplannen.	*Als beleggingsonderneming dient u te beschikken over bedrijfscontinuïteitsplannen, waarin ook de uitbestedingen worden meegenomen.*
49.	In bedrijfscontinuïteitsplannen wordt rekening gehouden met de mogelijkheid dat de kwaliteit van het verrichten van de uitbestede kritieke of belangrijke functie tot een onaanvaardbaar niveau verslechtert of in het geheel niet meer wordt uitgevoerd. Ook wordt daarin rekening gehouden met de mogelijke gevolgen van insolventie of andere vormen van falen van dienstverleners en, waar relevant, politieke risico's in het rechtsgebied van de dienstverlener.	*Ter informatie/geen opmerkingen*
	10. Interne auditfunctie	
50.	De activiteiten van de interne auditfunctie omvatten, op grond van een op risico's gebaseerde aanpak, een onafhankelijke toetsing van uitbestede activiteiten. Het auditplan en - programma behelzen in het bijzonder de uitbestedingsregelingen voor kritieke of belangrijke functies.	*Ter informatie/geen opmerkingen*
51.	Wat betreft het uitbestedingsproces zorgt de interne auditfunctie ten minste voor het volgende: a. dat het kader van de instelling of betalingsinstelling voor uitbesteding, inclusief het uitbestedingsbeleid, correct en doeltreffend wordt uitgevoerd en in overeenstemming is met de toepasselijke wet- en regelgeving, de risicostrategie en de beslissingen van het leidinggevend orgaan; b. dat de beoordeling van het kritieke karakter of het belang van de functies adequaat, kwalitatief goed en effectief is; c. dat de risicobeoordeling van uitbestedingsregelingen adequaat, kwalitatief goed en effectief is en dat de risico's in overeenstemming met de risicostrategie van de instelling blijven; d. de passende betrokkenheid van bestuursorganen; en e. dat uitbestedingsregelingen passend worden bewaakt en beheerd.	*Ter informatie/geen opmerkingen*
	11. Documentatievereisten	

52.	Als onderdeel van hun kader voor risicobeheer houden instellingen een register bij met informatie over alle uitbestedingsregelingen van de instelling en, indien van toepassing, op gesubconsolideerd en geconsolideerd niveau, zoals vermeld in hoofdstuk 2. Zij documenteren alle huidige uitbestedingsregelingen op correcte wijze, waarbij een onderscheid wordt gemaakt tussen de uitbesteding van kritieke of belangrijke functies en andere uitbestedingsregelingen. Met inachtneming van de nationale wetgeving bewaren instellingen gedurende een passende periode de documentatie met betrekking tot beëindigde uitbestedingsregelingen in het register en de ondersteunende documentatie.	*Zie tevens paragraaf 4.7 van de Blanco-paper*
53.	Met inachtneming van titel I van deze richtsnoeren en onder de voorwaarden van punt 23, onder d), kan het register als het gaat om instellingen en betalingsinstellingen binnen een groep, instellingen die blijvend bij een centraal orgaan zijn aangesloten, of instellingen die tot hetzelfde institutionele protectiestelsel behoren, centraal worden beheerd.	*Zie tevens paragraaf 4.7 van de Blanco-paper*
54.	Het register bevat ten minste de volgende informatie over alle bestaande uitbestedingsregelingen: a. een referentienummer voor elke uitbestedingsregeling; b. de aanvangsdatum en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, de einddatum en/of opzeggingstermijnen voor de dienstverlener en voor de instelling of betalingsinstelling; c. een korte beschrijving van de uitbestede functie, inclusief de gegevens die worden uitbesteed en of persoonsgegevens al dan niet zijn overgedragen (bijv. door ja of nee in een afzonderlijk gegevensveld te vermelden), of dat de verwerking daarvan aan een dienstverlener wordt uitbesteed; d. een door de instelling of betalingsinstelling toegewezen categorie die de aard van de functie als beschreven onder c) weerspiegelt (bijv. informatietechnologie (IT), controlefunctie), waardoor de inventarisatie van verschillende soorten regelingen gemakkelijker wordt; e. de naam van de dienstverlener, het handelsregisternummer, de identificatiecode voor de rechtspersoon (indien beschikbaar), het geregistreerde adres en andere relevante contactgegevens, en de naam van de moederonderneming (indien aanwezig); f. het land of de landen waar de dienst wordt verricht, inclusief de locatie (d.w.z. land of regio) van de gegevens; g. of de uitbestede functie al dan niet (ja/nee) als kritiek of belangrijk wordt beschouwd, plus, indien van toepassing, een korte samenvatting van de redenen waarom de uitbestede functie als kritiek of belangrijk wordt beschouwd; h. in het geval van uitbesteding aan een aanbieder van clouddiensten, de modellen voor de clouddiensten en de uitrol van de cloud, d.w.z. publiek/privaat/hybride/gemeenschappelijk, en de specifieke aard van de te bewaren gegevens en de locaties (d.w.z. landen of regio's) waar die gegevens worden opgeslagen; i. de datum waarop het kritieke karakter of het belang van de uitbestede functie voor het laatst zijn beoordeeld.	*Zie tevens paragraaf 4.7 van de Blanco-paper*

55.	Met het oog op de uitbesteding van kritieke of belangrijke functies bevat het register ten minste de volgende aanvullende informatie: a. de instellingen, betalingsinstellingen en andere ondernemingen binnen de prudentiële consolidatie of het institutionele protectiestelsel, indien van toepassing, die van de uitbesteding gebruikmaken; b. of de dienstverlener of onderdienstverlener deel uitmaakt van de groep of bij het institutionele protectiestelsel is aangesloten of het eigendom is van instellingen of betalingsinstellingen binnen de groep of het eigendom is van de leden van een institutioneel protectiestelsel; c. de datum waarop voor het laatst een risicobeoordeling heeft plaatsgevonden, en een korte samenvatting van de belangrijkste resultaten; d. de persoon of het besluitvormingsorgaan (bijv. het leidinggevend orgaan) in de instelling of de betalingsinstelling die de uitbestedingsregeling heeft goedgekeurd; e. de wetgeving die op de uitbestedingsregeling van toepassing is; f. de data van de meest recente en volgende geplande audits, indien van toepassing. g. indien van toepassing, de namen van onderaannemers waaraan materiële onderdelen van een kritieke of belangrijke functie zijn onderuitbesteed, inclusief het land waar de onderaannemers zijn geregistreerd, waar de dienst zal worden verricht en, indien van toepassing, de locatie (d.w.z. land of regio) waar de gegevens zullen worden opgeslagen; h. de uitkomsten van de beoordeling van de vervangbaarheid van de dienstverlener (als gemakkelijk, moeilijk of onmogelijk), de mogelijkheid om een kritieke of belangrijke functie opnieuw in de instelling of de betalingsinstelling te integreren of het effect van het beëindigen van de kritieke of belangrijke functie; i. alternatieve dienstverleners in overeenstemming met h); j. of de uitbestede kritieke of belangrijke functie tijdgevoelige bedrijfsactiviteiten ondersteunt; k. de geraamde jaarlijkse begrotingskosten.	*Zie tevens paragraaf 4.7 van de Blanco-paper*
56.	Instellingen en betalingsinstellingen stellen op verzoek het volledige register van alle bestaande uitbestedingsregelingen of gespecificeerde gedeelten daarvan beschikbaar, zoals informatie over alle uitbestedingsregelingen die onder een van de categorieën vallen als bedoeld in punt 54, onder d), van deze richtsnoeren (bijv. alle IT-uitbestedingsregelingen). Instellingen en betalingsinstellingen verstrekken deze informatie in een verwerkbare elektronische vorm (bijv. een veel gebruikt databankformaat, door komma's gescheiden waarden).	*Ter informatie/geen opmerkingen*
57.	Instellingen en betalingsinstellingen stellen op verzoek aan de bevoegde autoriteit alle informatie beschikbaar die nodig is om de bevoegde autoriteit in staat te stellen op doeltreffende wijze toezicht op de instelling of de betalingsinstelling te houden, waaronder indien nodig een kopie van de uitbestedingsovereenkomst.	*Ter informatie/geen opmerkingen*
58.	Instellingen, onverminderd artikel 19, lid 6, van Richtlijn (EU) 2015/2366, en betalingsinstellingen brengen de bevoegde autoriteiten naar behoren en tijdig op de hoogte van of gaan met de bevoegde autoriteiten een toezichtsdialoog aan over de geplande uitbesteding van kritieke of belangrijke functies en/of wanneer een uitbestede functie kritiek of belangrijk is geworden, en verschaffen ten minste de in punt 54 vermelde informatie.	*Zie tevens paragraaf 4.5 van de Blanco-paper*
59.	Instellingen en betalingsinstellingen informeren de bevoegde autoriteiten tijdig over materiële wijzigingen en/of ernstige gebeurtenissen in verband met hun uitbestedingsregelingen die grote gevolgen kunnen hebben voor het voorzetten van de bedrijfsactiviteiten van de instellingen of betalingsinstellingen.	*Zie tevens paragraaf 4.5 van de Blanco-paper*

60.	Instellingen en betalingsinstellingen documenteren naar behoren de beoordelingen op grond van titel IV en de resultaten van hun doorlopende bewakingsactiviteiten (bijv. prestaties van de dienstverlener, naleving van overeengekomen dienstverleningsniveaus, andere contractuele en regelgevingsvereisten, actualisering van de risicobeoordeling).	*Ter informatie/geen opmerkingen*
	Titel IV – Uitbestedingsproces	
	12.Analyse vóór uitbesteding	
61.	Alvorens een uitbestedingsregeling te treffen, handelen instellingen en betalingsinstellingen als volgt: a. Zij beoordelen of de uitbestedingsregeling een kritieke of belangrijke functie betreft, zoals beschreven in titel II. b. Zij beoordelen of aan de toezichtsvoorwaarden voor uitbesteding als vermeld in paragraaf 12.1 is voldaan. c. Zij identificeren en beoordelen alle relevante risico's van de uitbestedingsregeling in overeenstemming met paragraaf 12.2. d. Zij voeren een passend due diligence-onderzoek uit ten aanzien van de mogelijke toekomstige dienstverlener in overeenstemming met paragraaf 12.3. e. Zij identificeren en beoordelen belangenconflicten die de uitbesteding kan veroorzaken, in overeenstemming met hoofdstuk 8.	*Zie tevens paragraaf 4.2 van de Blanco-paper*
	12.1 Toezichtsvoorwaarden voor uitbesteding	
62.	Instellingen en betalingsinstellingen zorgen ervoor dat de uitbesteding van functies van bankactiviteiten of betalingsdiensten, voor zover voor de uitvoering van die functie een vergunning van of registratie door een bevoegde autoriteit is vereist in de lidstaat waar zij zijn toegelaten, aan een dienstverlener in dezelfde of een andere lidstaat alleen dan plaatsvindt als aan een van de volgende voorwaarden wordt voldaan: a. De dienstverlener heeft een vergunning van of is geregistreerd door een bevoegde autoriteit om zulke bankactiviteiten of betalingsdiensten te verrichten. Of b. De dienstverlener heeft anderszins toestemming ontvangen om deze bankactiviteiten of betalingsdiensten in overeenstemming met het relevante nationale wettelijke kader uit te voeren.	*Niet van toepassing voor beleggingsondernemingen*

63.	Instellingen en betalingsinstellingen zorgen ervoor dat de uitbesteding van functies van bankactiviteiten of betalingsdiensten, voor zover voor de uitvoering van die functie een vergunning of registratie door een bevoegde autoriteit is vereist in de lidstaat waar zij zijn toegelaten, aan een dienstverlener in een derde land alleen dan plaatsvindt als aan de volgende voorwaarden wordt voldaan: a. De dienstverlener heeft een vergunning of is geregistreerd om die bankactiviteit of betalingsdienst in het derde land te verrichten en staat onder toezicht van een relevante bevoegde autoriteit in dat derde land ("toezichthoudende autoriteit" genoemd). b. Er bestaat een passende samenwerkingsovereenkomst, bijv. in de vorm van een memorandum van overeenstemming of collegeovereenkomst tussen de bevoegde autoriteiten die voor het toezicht op de instelling verantwoordelijk zijn, en de toezichthoudende autoriteiten die belast zijn met het toezicht op de dienstverlener. En c. De samenwerkingsovereenkomst waarvan sprake is onder b), waarborgt dat de bevoegde autoriteiten ten minste in staat zijn om: i. op verzoek de informatie te verkrijgen die noodzakelijk is voor het uitvoeren van hun toezichtstaken krachtens Richtlijn 2013/36/EU, Verordening (EU) nr. 575/2013, Richtlijn (EU) 2015/2366 en Richtlijn 2009/110/EG; ii. passende toegang te krijgen tot gegevens, documenten, locaties of personeel in het derde land die van belang zijn voor de uitoefening van hun toezichtsbevoegdheden; iii. zo spoedig mogelijk informatie van de toezichthoudende autoriteit in het derde land te ontvangen voor het onderzoeken van kennelijke schendingen van de vereisten van Richtlijn 2013/36/EU, Verordening (EU) nr. 575/2013, Richtlijn (EU) 2015/2366 en Richtlijn 2009/110/EG; en iv. met de relevante toezichthoudende autoriteiten in het derde land samen te werken in het kader van handhavingsacties bij schendingen van de toepasselijke regelgevingsvereisten en de nationale wetgeving in de lidstaat. Bij de samenwerking hoort het onder meer, maar niet per se uitsluitend, te gaan om het ontvangen van informatie over mogelijke schendingen van de toepasselijke regelgevingsvereisten van de toezichthoudende autoriteiten in het derde land, zodra dit praktisch mogelijk is.	*Niet van toepassing voor beleggingsondernemingen*
	12.2 Beoordeling van risico's van uitbestedingsregelingen	
64.	Instellingen en betalingsinstellingen beoordelen de mogelijke gevolgen van uitbestedingsregelingen voor hun operationele risico, houden rekening met de beoordelingsresultaten wanneer zij besluiten of de functie aan een dienstverlener wordt uitbesteed, en nemen passende maatregelen om onnodige aanvullende operationele risico's te voorkomen voordat zij uitbestedingsregelingen aangaan.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
65.	De beoordeling omvat, waar nodig, scenario's van mogelijke risicogebeurtenissen, inclusief zeer ernstige operationele risicogebeurtenissen. Binnen de scenarioanalyse beoordelen instellingen en betalingsinstellingen de mogelijke gevolgen van falende of ontoereikende diensten, inclusief de risico's die worden veroorzaakt door processen, systemen, mensen of externe gebeurtenissen. Instellingen en betalingsinstellingen documenteren, met inachtneming van het evenredigheidsbeginsel als bedoeld in hoofdstuk 1, de verrichte analyse en de uitkomsten daarvan en maken een raming van de mate waarin hun operationele risico door de uitbestedingsregeling zou toenemen of afnemen. Met inachtneming van titel I mogen kleine en niet-complexe instellingen en betalingsinstellingen een kwalitatieve aanpak van risicobeoordeling hanteren, terwijl grote of complexe instellingen een meer verfijnde benadering dienen te hebben, waaronder, indien beschikbaar, het gebruik van interne en externe verliesgegevens als informatiebron voor de scenarioanalyse.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*

66.	Bij de risicobeoordeling houden instellingen en betalingsinstellingen ook rekening met de verwachte baten en lasten van de voorgestelde uitbestedingsregeling, inclusief het afwegen van risico's die kunnen worden verkleind of beter beheerd, tegen risico's die uit de voorgestelde uitbestedingsregeling kunnen voortvloeien. Zij kijken daarbij ten minste naar: a. concentratierisico's, inclusief als gevolg van: i. uitbesteding aan een dominante dienstverlener die niet gemakkelijk kan worden vervangen; en ii. meerdere uitbestedingsregelingen met dezelfde dienstverlener of dienstverleners die nauw met elkaar verbonden zijn; b. de geaggregeerde risico's als gevolg van de uitbesteding van diverse functies binnen de gehele instelling of betalingsinstelling en, in het geval van groepen instellingen of institutionele protectiestelsels, de geaggregeerde risico's op geconsolideerde basis of op basis van het institutionele protectiestelsel; c. in het geval van belangrijke instellingen het instaprisico, d.w.z. het risico dat kan voortvloeien uit de noodzaak om een dienstverlener in nood financieel te ondersteunen of zijn bedrijfsactiviteiten over te nemen; en d. de maatregelen die de instelling of betalingsinstelling en de dienstverlener hebben getroffen om de risico's te beheren en te beperken.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
67.	Wanneer het op grond van de uitbestedingsregeling mogelijk is dat de dienstverlener kritieke of belangrijke functies aan andere dienstverleners onderuitbesteedt, houden instellingen en betalingsinstellingen rekening met: a. de risico's van onderuitbesteding, inclusief de aanvullende risico's die zich kunnen voordoen als de onderaannemer in een derde land of een ander land dan de dienstverlener is gevestigd; b. het risico dat door lange en complexe ketens van onderuitbesteding instellingen of betalingsinstellingen minder goed in staat zijn toezicht op de uitbestede kritieke of belangrijke functie te houden en bevoegde autoriteiten minder goed toezicht op deze instellingen kunnen uitoefenen.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*

68.	Bij het beoordelen van de risico's vóór uitbesteding en tijdens de continue bewaking van de prestaties van de dienstverlener, verrichten instellingen en betalingsinstellingen in elk geval de volgende handelingen: a. Zij inventariseren de relevante functies en de bijbehorende gegevens en systemen en delen deze in naar gevoeligheid en benodigde veiligheidsmaatregelen. b. Zij verrichten een grondige op risico's gebaseerde analyse van de functies en de bijbehorende gegevens en systemen die zij overwegen uit te besteden of hebben uitbesteed, en pakken de potentiele risico's aan, vooral de operationele risico's, inclusief juridische, ICT-, nalevings- en reputatierisico's, en de beperkingen van het toezicht in verband met de landen waar de uitbestede diensten (waarschijnlijk) worden verleend en waar de gegevens (waarschijnlijk) worden opgeslagen. c. Zij gaan na welke gevolgen de vestigingsplaats van de dienstverlener heeft (binnen of buiten de EU). d. Zij kijken naar de politieke stabiliteit en de veiligheid in de betrokken rechtsgebieden, waaronder: i. de geldende wetgeving, inclusief wetten over gegevensbescherming; ii. de bestaande voorzieningen voor rechtshandhaving; en iii. het insolventierecht dat van toepassing zou zijn bij niet-naleving door een dienstverlener en de mogelijke beperkingen die zich zouden voordoen bij een urgent herstel van de gegevens van de instelling of betalingsinstelling in het bijzonder. e. Zij definiëren, en nemen besluiten over, passende bescherming van de vertrouwelijkheid van gegevens, de continuïteit van de uit te besteden activiteiten, en de integriteit en herleidbaarheid van gegevens en systemen in het kader van de voorgenomen uitbesteding. Verder gaan instellingen en betalingsinstellingen na of er specifieke maatregelen nodig zijn voor gegevens in transit, opgeslagen gegevens en gegevens in rusttoestand, zoals de toepassing van versleutelingstechnieken (encryptie) in combinatie met een passende opzet voor sleutelbeheer. f. Zij bekijken of de dienstverlener een dochteronderneming of moederonderneming van de instelling is, binnen de boekhoudkundige consolidatie van de instelling valt of lid of eigendom is van instellingen die bij een institutioneel protectiestelsel zijn aangesloten en, zo ja, in hoeverre de instelling zeggenschap over de dienstverlener heeft of diens handelingen kan beïnvloeden in lijn met hoofdstuk 2.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
	12.3 Due diligence	
69.	Alvorens een uitbestedingsregeling aan te gaan en naar de operationele risico's te kijken die met de uit te besteden functie verband houden, zien instellingen en betalingsinstellingen er tijdens hun selectie- en beoordelingsprocedure op toe dat de dienstverlener geschikt is.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
70.	Wat betreft kritieke en belangrijke functies zien instellingen en betalingsinstellingen erop toe dat de dienstverlener de bedrijfsreputatie, passende en toereikende bekwaamheden, de deskundigheid, de capaciteit, de middelen (bijv. personeel, IT, financieel), de organisatiestructuur en, indien van toepassing, de vereiste wettelijke vergunning(en) of registratie(s) heeft om de kritieke of belangrijke functie op betrouwbare en professionele wijze te verrichten zodat deze tijdens de loop van het conceptcontract aan zijn verplichtingen kan voldoen.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*

71.	Aanvullende factoren die bij het verrichten van een due diligence-onderzoek naar een potentiële dienstverlener in ogenschouw worden genomen, zijn onder meer, zonder hiertoe beperkt te zijn: a. zijn bedrijfsmodel, karakter, omvang, complexiteit, financiële situatie, eigendoms- en groepsstructuur; b. de langdurige relaties met dienstverleners die reeds zijn beoordeeld en die diensten voor de instelling of betalingsinstelling verrichten; c. of de dienstverlener een moederonderneming of dochteronderneming van de instelling of betalingsinstelling is, binnen de boekhoudkundige consolidatie van de instelling valt of lid of eigendom is van instellingen die bij hetzelfde institutionele protectiestelsel zijn aangesloten als waartoe de instelling behoort; d. of de dienstverlener al dan niet onder toezicht van de bevoegde autoriteiten staat	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
72.	Wanneer de uitbesteding ook het verwerken van persoonsgegevens of vertrouwelijke gegevens betreft, vergewissen instellingen en betalingsinstellingen zich ervan dat de dienstverlener passende technische en organisatorische maatregelen neemt om de gegevens te beschermen.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
73.	Instellingen en betalingsinstellingen zetten de nodige stappen om ervoor te zorgen dat dienstverleners handelen op een wijze die strookt met hun waarden en gedragscode. Met name wat betreft dienstverleners in derde landen en, indien van toepassing, hun onderaannemers, vergewissen instellingen en betalingsinstellingen zich ervan dat de dienstverlener op een ethische en maatschappelijk verantwoorde wijze handelt en zich houdt aan de internationale normen op het gebied van mensenrechten (bijv. het Europees Verdrag voor de rechten van de mens), milieubescherming en passende arbeidsomstandigheden, inclusief het verbod op kinderarbeid.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
	13. Contractfase	
74.	De rechten en plichten van de instelling, de betalingsinstelling en de dienstverlener worden duidelijk afgebakend en in een schriftelijke overeenkomst vastgelegd.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
75.	De uitbestedingsovereenkomst voor kritieke of belangrijke functies behelst ten minste het volgende: a. een heldere beschrijving van de te verrichten uitbestede functie; b. de aanvangsdatum en einddatum, indien van toepassing, van de overeenkomst en de opzeggingstermijnen voor de dienstverlener en de instelling of betalingsinstelling; c. de wetgeving die op de overeenkomst van toepassing is; d. de financiële verplichtingen van de partijen; e. of de onderuitbesteding van een kritieke of belangrijke functie, of materiële onderdelen daarvan, is toegestaan en zo ja, de in paragraaf 13.1 vermelde voorwaarden die voor de onderuitbesteding gelden; f. de locatie(s) (d.w.z. regio's of landen) waar de kritieke of belangrijke functie zal worden verricht en/of waar de relevante gegevens zullen worden bewaard en verwerkt, inclusief de mogelijke opslaglocatie, en de voorwaarden waaraan moet worden voldaan, met inbegrip van de vereiste om de instelling of betalingsinstelling in kennis te stellen als de dienstverlener voorstelt de locatie(s) te wijzigen; g. waar relevant, bepalingen inzake de toegankelijkheid, beschikbaarheid, integriteit, privacy en veiligheid van de betrokken gegevens, als vermeld in paragraaf 13.2; h. het recht van de instelling of betalingsinstelling om de prestaties van de dienstverlener doorlopend te bewaken; i. de overeengekomen niveaus van dienstverlening, die nauwkeurige kwantitatieve en kwalitatieve prestatiedoelen voor de uitbestede functie omvatten om tijdige bewaking mogelijk te maken, zodat zonder onnodig uitstel passende corrigerende maatregelen kunnen worden genomen als de	*Zie tevens paragraaf 4.4 van de Blanco-paper*

	overeengekomen dienstverleningsniveaus niet worden gehaald; j. de verplichtingen van de dienstverlener betreffende rapportage aan de instelling of betalingsinstelling, inclusief het melden door de dienstverlener van elke ontwikkeling die materiële gevolgen kan hebben voor het vermogen van de dienstverlener om de kritieke of belangrijke functie doeltreffend uit te voeren in lijn met de overeengekomen dienstverleningsniveaus en conform de toepasselijke wet- en regelgeving en, indien van toepassing, de verplichting om verslagen van de interne auditfunctie van de dienstverlener te overleggen; k. of de dienstverlener zich verplicht tegen bepaalde risico's dient te verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking; l. de vereiste om bedrijfsnoodplannen ten uitvoer te leggen en te testen; m. bepalingen die ervoor zorgen dat toegang kan worden verkregen in de gegevens die het eigendom van de instelling of betalingsinstelling zijn, wanneer de dienstverlener insolvent is, zich in een afwikkelingsproces bevindt of zijn bedrijfsactiviteiten beëindigt; n. de verplichting van de dienstverlener om met de bevoegde autoriteiten en afwikkelingsautoriteiten van de instelling of betalingsinstelling samen te werken, met inbegrip van andere personen die door hen zijn aangewezen; o. voor instellingen een duidelijke verwijzing naar de bevoegdheden van de nationale afwikkelingsautoriteit, vooral naar de artikelen 68 en 71 van Richtlijn 2014/59/EU (BRRD), en met name een beschrijving van de "materiële verplichtingen" van het contract in de zin van artikel 68 van die richtlijn; p. het onbeperkte recht van instellingen, betalingsinstellingen en bevoegde autoriteiten om de dienstverlener te inspecteren en te controleren, vooral als het gaat om de kritieke of belangrijke uitbestede functie, als vermeld in paragraaf 13.3; q. beëindigingsrechten, als vermeld in paragraaf 13.4.	
	13.1 Onderuitbesteding van kritieke of belangrijke functies	
76.	In de uitbestedingsovereenkomst wordt aangegeven of de onderuitbesteding van kritieke of belangrijke functies, of materiële onderdelen daarvan, al dan niet is toegestaan.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
77.	Als de onderuitbesteding van kritieke of belangrijke functies is toegestaan, bepalen instellingen en betalingsinstellingen of het deel van de functie dat wordt onderuitbesteed, als zodanig kritiek of belangrijk (d.w.z. een materieel onderdeel van van de kritieke of belangrijke functie) is. Indien dat het geval is, leggen zij dit in het register vast.	*Zie tevens paragraaf 4.4 van de Blanco-paper*

78.	Als de onderuitbesteding van kritieke of belangrijke functies is toegestaan, worden aan de schriftelijke overeenkomst de volgende eisen gesteld: a. Alle soorten activiteiten die van onderuitbesteding zijn uitgesloten, worden erin vermeld. b. De voorwaarden waaraan in het geval van onderuitbesteding moet worden voldaan, worden erin vermeld. c. Er moet in worden aangegeven dat de dienstverlener verplicht is toezicht te houden op diensten die hij heeft onderuitbesteed, om ervoor te zorgen dat de contractuele verplichtingen tussen de dienstverlener en de instelling of betalingsinstelling voortdurend worden nagekomen. d. Op grond van de overeenkomst moet de dienstverlener voorafgaande specifieke of algemene schriftelijke toestemming van de instelling of betalingsinstelling krijgen alvorens tot onderuitbesteding van de gegevens over te gaan. e. Zij omvat een verplichting voor de dienstverlener om de instelling of betalingsinstelling te informeren over elke geplande onderuitbesteding, of materiële wijzigingen daarin, met name wanneer de dienstverlener zijn verantwoordelijkheden op grond van de uitbestedingsovereenkomst daardoor minder goed kan vervullen. Dit behelst ook geplande belangrijke wijzigingen wat betreft onderaannemers en de kennisgevingstermijn; in het bijzonder wordt de kennisgevingstermijn zodanig vastgesteld dat de uitbestedende instelling of betalingsinstelling ten minste de risico's van de voorgestelde wijzigingen kan beoordelen en bezwaar kan maken tegen wijzigingen voordat de geplande onderuitbesteding, of materiële wijzigingen daarin, plaatsvinden. f. Waar nodig wordt in de overeenkomst bepaald dat de instelling of betalingsinstelling het recht heeft bezwaar te maken tegen een beoogde onderuitbesteding, of materiële wijzigingen daarin, of dat expliciete goedkeuring is vereist. g. In de overeenkomst wordt bepaald dat de instelling of betalingsinstelling contractueel gerechtigd is de overeenkomst in het geval van onnodige onderuitbesteding te beëindigen, bijvoorbeeld wanneer door de onderuitbesteding de risico's voor de instelling of betalingsinstelling materieel of als de dienstverlener tot onderuitbesteding overgaat zonder de instelling of betalingsinstelling daarvan in kennis te stellen.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
79.	Instellingen en betalingsinstellingen stemmen alleen met onderuitbesteding in als de onderaannemer zich ertoe verbindt: a. aan alle toepasselijke wetten, regelgevingsvereisten en contractuele verplichtingen te voldoen; en b. aan de instelling, betalingsinstelling en bevoegde autoriteit dezelfde contractuele toegangs- en auditrechten als aan de dienstverlener toe te kennen.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
	13.2. Beveiliging van gegevens en systemen	
81.	Instellingen en betalingsinstellingen zorgen ervoor dat dienstverleners, waar relevant, aan de juiste IT-beveiligingsnormen voldoen.	*Zie tevens paragraaf 4.3 en 4.4 van de Blanco-paper*
82.	Waar relevant (bijv. in het kader van de uitbesteding van cloud- of andere ICT-diensten) stellen instellingen en betalingsinstellingen in de uitbestedingsovereenkomst eisen voor de beveiliging van gegevens en systemen vast en zien zij er voortdurend op toe dat deze eisen worden nageleefd.	*Ter informatie/geen opmerkingen*
83.	In het geval van uitbesteding aan aanbieders van clouddiensten en andere uitbestedingsregelingen die gaan over de verwerking of doorgifte van persoonsgegevens of vertrouwelijke gegevens, hanteren instellingen en betalingsinstellingen een op risico's gebaseerde aanpak met betrekking tot de locatie(s) van gegevensopslag en -verwerking (d.w.z. land of regio) en overwegingen over de beveiliging van informatie.	*Zie tevens paragraaf 4.3 en 4.4 van de Blanco-paper*

84.	Onverminderd de voorschriften van Verordening (EU) 2016/679 houden instellingen en betalingsinstellingen bij uitbesteding (vooral naar derde landen) rekening met verschillen in nationale bepalingen over de bescherming van gegevens. Instellingen en betalingsinstellingen zorgen ervoor dat in de uitbestedingsovereenkomst wordt bepaald dat de dienstverlener vertrouwelijke, persoonlijke of anderszins gevoelige informatie moet beschermen en moet voldoen aan alle wettelijke vereisten betreffende de bescherming van gegevens die voor de instelling of betalingsinstelling gelden (bijv. de bescherming van persoonsgegevens en dat het bankgeheim of soortgelijke wettelijke geheimhoudingsverplichtingen met betrekking tot de informatie van cliënten, indien van toepassing, in acht worden genomen).	*Zie tevens paragraaf 4.3 en 4.4 van de Blanco-paper*
	13.3. Toegangs-, informatie- en auditrechten	
85.	Instellingen en betalingsinstellingen leggen in de schriftelijke uitbestedingsregeling vast dat de interne auditfunctie de uitbestede functie via een op risico's gebaseerde benadering kan toetsen	*Zie tevens paragraaf 4.4 van de Blanco-paper*
86.	De schriftelijke uitbestedingsregelingen tussen instellingen en dienstverleners verwijzen, ongeacht het kritieke karakter of het belang van de uitbestede functie, naar de bevoegdheden van bevoegde autoriteiten en afwikkelingsautoriteiten inzake informatievergaring en onderzoek krachtens artikel 63, lid 1, onder a), van Richtlijn 2014/59/EU en artikel 65, lid 3, van Richtlijn 2013/36/EU wat betreft dienstverleners in een lidstaat, en waarborgen deze rechten ook wat betreft dienstverleners in derde landen.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
87.	Als het gaat om de uitbesteding van kritieke of belangrijke functies leggen instellingen en betalingsinstellingen in de schriftelijke uitbestedingsovereenkomst vast dat de dienstverlener aan hen en hun bevoegde autoriteiten, inclusief afwikkelingsautoriteiten, en aan iedere andere persoon die door hen of de bevoegde autoriteiten is aangewezen: a. volledige toegang verleent tot alle relevante bedrijfslocaties (bijv. hoofdkantoren en operationele centra), inclusief het volledige scala aan relevante apparatuur, systemen, netwerken, informatie en gegevens die worden gebruikt om de uitbestede functie te verrichten, waaronder bijbehorende financiële informatie, personeel en de externe auditors van de dienstverlener ("toegangs- en informatierechten"); en b. een onbeperkt recht van inspectie en audits verleent met betrekking tot de uitbestedingsregeling ("auditrechten") om hen in staat te stellen de uitbestedingsregeling te bewaken en ervoor te zorgen dat aan alle toepasselijke regelgeving en contractuele voorschriften wordt voldaan.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
88.	Wat betreft de uitbesteding van functies die niet kritiek of belangrijk zijn, waarborgen instellingen en betalingsinstellingen de in punt 87, onder a) en b), en in paragraaf 13.3 vermelde toegangs- en auditrechten via een op risico's gebaseerde aanpak, met inachtneming van de aard van de uitbestede functie en de bijbehorende operationele en reputatierisico's, de schaalbaarheid ervan, de mogelijke gevolgen voor de permanente uitvoering van de activiteiten in verband met de functie, en de contractperiode. Instellingen en betalingsinstellingen houden er rekening mee dat functies in de loop van de tijd kritiek of belangrijk kunnen worden.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
89.	Instellingen en betalingsinstellingen zorgen ervoor dat de uitbestedingsovereenkomst of enige andere contractuele regeling de doeltreffende uitoefening van de toegangs- en auditrechten niet in de weg staat of beperkt; deze rechten kunnen worden uitgeoefend door henzelf, door bevoegde autoriteiten of door derden die zij hebben aangewezen om deze rechten uit te oefenen.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
90.	Instellingen en betalingsinstellingen oefenen hun toegangs- en auditrechten uit, bepalen via een op risico's gebaseerde aanpak de frequentie van de audits en de gebieden die aan een audit moeten worden onderworpen, en houden zich aan relevante, algemeen aanvaarde, nationale en internationale auditnormen	*Ter informatie/geen opmerkingen*

91.	Onverminderd hun eindverantwoordelijkheid voor uitbestedingsregelingen kunnen instellingen en betalingsinstellingen gebruikmaken van: a. gemeenschappelijke audits die samen met andere cliënten van dezelfde dienstverlener worden georganiseerd en door hen en deze cliënten of een door hen aangestelde derde worden uitgevoerd om de auditmiddelen doelmatiger te gebruiken en de organisatorische last voor de cliënten en de dienstverlener te verminderen; b. door de dienstverlener verstrekte externe certificeringen en externe of interne auditverslagen.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
92.	Wat betreft de uitbesteding van kritieke of belangrijke functies beoordelen instellingen en betalingsinstellingen of de externe certificeringen en verslagen als bedoeld in punt 91, onder b), adequaat en voldoende zijn om aan hun regelgevingsverplichtingen te voldoen, en vertrouwen zij op termijn niet uitsluitend op deze verslagen.	*Ter informatie/geen opmerkingen*
93.	Instellingen en betalingsinstellingen hanteren de methode als bedoeld in punt 91, onder b), alleen dan als zij: a. tevreden zijn over het auditplan voor de uitbestede functie; b. erop toezien dat de certificering of het auditverslag betrekking heeft op de systemen (d.w.z. processen, applicaties, infrastructuur, datacentra, enz.) en controles die door de instelling of betalingsinstelling als essentieel zijn aangemerkt, en de naleving van de relevante regelgevingsvereisten; c. de certificering of het auditverslag continu grondig beoordelen en nagaan of de verslagen of certificeringen niet verouderd zijn; d. erop toezien dat ook toekomstige versies van de certificering of het auditverslag betrekking hebben op essentiële systemen en controles; e. tevreden zijn over de geschiktheid van de certificerende of controlerende partij (bijv. met betrekking tot roulering van de certificerende of controlerende organisatie, kwalificaties, deskundigheid, herhaling van de uitvoering / controle van bewijsstukken in het betrokken auditdossier); f. zich ervan hebben vergewist dat de certificeringen zijn afgegeven en de audits zijn uitgevoerd overeenkomstig algemeen aanvaarde professionele normen en dat zij een toetsing omvatten van de operationele doeltreffendheid van de aanwezige essentiële controles; g. contractueel gerechtigd zijn te verzoeken om uitbreiding van de reikwijdte van de certificering of het auditverslag tot andere relevante systemen en controles; het aantal en de frequentie van dergelijke verzoeken dienen redelijk te zijn en vanuit het oogpunt van risicobeheer gerechtvaardigd zijn; en h. het contractuele recht behouden om naar eigen inzicht afzonderlijke audits met betrekking tot de uitbesteding van kritieke of belangrijke functies uit te voeren.	*Ter informatie/geen opmerkingen*
94.	Conform de EBA-richtsnoeren inzake de beoordeling van het ICT-risico in het kader van SREP zorgen instellingen, waar relevant, ervoor dat zij periodieke penetratietests kunnen uitvoeren om te beoordelen hoe effectief de ten uitvoer gelegde cyber- en interne ICT-veiligheidsmaatregelen en -processen zijn. Met inachtneming van titel 1 beschikken betalingsinstellingen eveneens over interne ICT-controlemechanismen, inclusief veiligheidscontrole en risicobeperkende maatregelen in verband met ICT.	*Blanco heeft (voor de KYC Suite) een doorlopend bug bounty programma bij HackerOne. Ethische hackers proberen dan de software van Blanco (binnen een gecontroleerde omgeving) binnen te dringen, wat een vergelijkbaar is met een penetratietest, maar dan doorlopend. Het HackerOne programma is in scope van de ISAE3402 certificering.*
95.	Vóór een gepland bezoek ter plaatse stellen instellingen, betalingsinstellingen, bevoegde autoriteiten en auditors of derden die namens de instelling, betalingsinstelling of bevoegde autoriteiten handelen, de dienstverleners een redelijke tijd van tevoren daarvan in kennis, tenzij dat vanwege een nood- of crisissituatie niet mogelijk is of zou leiden tot een situatie waarin de audit niet langer doeltreffend zou zijn.	*Ter informatie/geen opmerkingen*

96.	Tijdens het verrichten van audits in een omgeving van meerdere cliënten worden risico's voor de omgeving van een andere cliënt (bijv. effect op dienstverleningsniveaus, beschikbaarheid van gegevens, vertrouwelijkheidsaspecten) vermeden of beperkt.	*Ter informatie/geen opmerkingen. Dit is altijd een belangrijke voorwaarde van Blanco voor het uitvoeren van een audit. Dit is ook goed mogelijk, gezien de gesegregeerde accounts.*
97.	Wanneer de uitbestedingsregeling technisch bijzonder complex is, bijvoorbeeld in het geval van uitbesteding van clouddiensten, gaat de instelling of betalingsinstelling na of degene die de audit uitvoert – haar eigen interne auditors, of de namens haar handelende pool van auditors of externe auditors – de juiste en relevante kennis en vaardigheden heeft om de desbetreffende audits en/of beoordelingen op doeltreffende wijze te verrichten. Hetzelfde geldt voor het personeel van de instelling of betalingsinstelling dat de externe certificering of de door dienstverleners verrichte audits toetst.	*Ter informatie/geen opmerkingen*
	13.4 Beëindigingsrechten	
98.	De uitbestedingsregeling biedt de instelling of betalingsinstelling uitdrukkelijk de mogelijkheid om de regeling in overeenstemming met de geldende wetgeving te beëindigen, waaronder in de volgende situaties: veiligheidsmaatregelen en -processen zijn. betalingsinstellingen eveneens over interne ICT-controlemechanismen, inclusief veiligheidscontrole en risicobeperkende maatregelen in verband met ICT. a. wanneer degene die de uitbestede functies verricht, de geldende wet- en regelgeving of contractuele bepalingen overtreedt; b. wanneer er belemmeringen worden geconstateerd waardoor het mogelijk is dat er veranderingen in de uitvoering van de uitbestede functie optreden; c. wanneer er sprake is van materiële wijzigingen die gevolgen hebben voor de uitbestedingsregeling of de dienstverlener (bijv. onderuitbesteding of wijzigingen wat betreft van onderaannemers); d. wanneer er zwakke punten zijn als het gaat om het beheer en de beveiliging van vertrouwelijke, persoonlijke of anderszins gevoelige gegevens of informatie; en e. wanneer de bevoegde autoriteit van de instelling of betalingsinstelling instructies geeft, bijvoorbeeld als de bevoegde autoriteit als gevolg van de uitbestedingsregeling niet langer in een positie is om doeltreffend toezicht op de instelling of betalingsinstelling te houden.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
99.	De uitbestedingsregeling faciliteert de overdracht van de uitbestede functie aan een andere dienstverlener of het opnieuw onderbrengen ervan bij de instelling of betalingsinstelling. Hiertoe dienen de volgende zaken in de schriftelijke uitbestedingsregeling te worden opgenomen: a. een heldere omschrijving van de verplichtingen van de bestaande dienstverlener, in het geval van een overdracht van de uitbestede functie aan een andere dienstverlener of weer terug aan de instelling of betalingsinstelling, inclusief de behandeling van gegevens; b. een passende overgangsperiode waarin de dienstverlener, na de beëindiging van de uitbestedingsregeling, de uitbestede functie blijft verrichten om het risico op verstoringen te beperken; en c. een verplichting voor de dienstverlener om de instelling of betalingsinstelling te helpen de functie op ordelijke wijze over te dragen wanneer de uitbestedingsovereenkomst wordt beëindigd.	*Zie tevens paragraaf 4.4 van de Blanco-paper*
	14. Toezicht op uitbestede functies	

100.	Instellingen en betalingsinstellingen bewaken voortdurend de prestaties van de dienstverleners met betrekking tot alle uitbestedingsregelingen via een op risico's gebaseerde aanpak, waarbij het accent vooral ligt op de uitbesteding van kritieke of belangrijke functies, onder meer in de zin dat de beschikbaarheid, integriteit en veiligheid van gegevens en informatie wordt gewaarborgd. Wanneer de risico, aard of omvang van een uitbestede functie op materiële punten is gewijzigd, beoordelen instellingen en betalingsinstellingen het kritieke karakter of het belang van die functie opnieuw conform hoofdstuk 4.	*Ter informatie/geen opmerkingen*
101.	Instellingen en betalingsinstellingen betrachten de nodige bekwaamheid, zorgvuldigheid en toewijding wanneer zij uitbestedingsregelingen bewaken en beheren.	*Ter informatie/geen opmerkingen*
102.	Instellingen werken hun risicobeoordeling regelmatig bij in overeenstemming met paragraaf 12.2 en brengen periodiek verslag uit aan het leidinggevend orgaan over de risico's die zij met betrekking tot de uitbesteding van kritieke of belangrijke functies hebben geïdentificeerd.	*Ter informatie/geen opmerkingen*
103.	Instellingen en betalingsinstellingen bewaken en beheren hun interne concentratierisico's die door uitbestedingsregelingen worden veroorzaakt, met inachtneming van paragraaf 12.2 van deze richtsnoeren.	*Ter informatie/geen opmerkingen*
104.	Instellingen en betalingsinstellingen zien er doorlopend op toe dat uitbestedingsregelingen conform hun beleid aan passende prestatie- en kwaliteitsnormen voldoen, waarbij het accent vooral ligt op uitbestede kritieke of belangrijke functies. Dit doen zij door: a. ervoor te zorgen dat zij passende verslagen van dienstverleners ontvangen; b. de prestaties van dienstverleners te beoordelen met behulp van instrumenten als kernprestatie-indicatoren, sleutelindicatoren voor risicobeheersing, dienstverleningsverslagen, zelfcertificering en onafhankelijke toetsingen; en c. alle andere relevante informatie van de dienstverlener te beoordelen, inclusief verslagen over maatregelen en tests op het gebied van de bedrijfscontinuïteit.	*Ter informatie/geen opmerkingen*
105.	Instellingen nemen de nodige maatregelen als zij tekortkomingen in het verrichten van de uitbestede functie constateren. Met name komen instellingen en betalingsinstellingen in actie wanneer er aanwijzingen zijn dat dienstverleners de uitbestede kritieke of belangrijke functie niet doeltreffend of niet in overeenstemming met de geldende wetten en regelgevingsvereisten uitvoeren. Als er tekortkomingen worden vastgesteld, nemen instellingen en betalingsinstellingen passende corrigerende of herstelmaatregelen. Zo nodig wordt de uitbestedingsovereenkomst met onmiddellijke ingang beëindigd.	*Ter informatie/geen opmerkingen*
	15. Exitstrategieën	
106.	Instellingen en betalingsinstellingen hebben tijdens de uitbesteding van kritieke of belangrijke functies een gedocumenteerde exitstrategie die in lijn is met hun uitbestedingsbeleid en hun bedrijfscontinuïteitsplannen; zij houden daarbij ten minste rekening met de mogelijkheid dat: a. uitbestedingsregelingen worden beëindigd; b. de dienstverlener faalt; c. de kwaliteit van de verrichte functie verslechtert en dat er sprake is of kan zijn van bedrijfsverstoringen die ontstaan doordat de functie niet of op onjuiste wijze wordt verricht; d. aanzienlijke risico's voor de passende en voortdurende uitvoering van de functie.	*Ter informatie/geen opmerkingen*

107.	Instellingen en betalingsinstellingen zorgen ervoor dat zij zich uit uitbestedingsregelingen kunnen terugtrekken zonder dat hun bedrijfsactiviteiten onnodig worden verstoord, zonder dat zij de regelgevingsvereisten minder goed naleven en zonder dat dit ten koste gaat van de continuïteit en kwaliteit van hun dienstverlening aan cliënten. Hiertoe: a. ontwikkelen en implementeren zij exitplannen die volledig, gedocumenteerd en waar nodig voldoende getoetst zijn (bijv. door de potentiële kosten, gevolgen, middelen en tijdsimplicaties te analyseren in verband met de overdracht van een uitbestede dienst aan een alternatieve dienstverlener); en b. zoeken zij alternatieve oplossingen en stellen zij overgangsplannen op waarmee de instelling of betalingsinstelling uitbestede functies en gegevens bij de dienstverlener kan weghalen en aan alternatieve dienstverleners of weer aan de instelling of betalingsinstelling kan overdragen, of waarmee zij andere maatregelen kunnen treffen om er beheerst en op voldoende beproefde wijze voor te kunnen zorgen dat de kritieke of belangrijke functie of bedrijfsactiviteit wordt voortgezet; hierbij houden zij rekening met de uitdagingen die zich kunnen voordoen vanwege de locatie van de gegevens en nemen zij de nodige maatregelen om tijdens de overgangsfase de bedrijfsactiviteit te waarborgen.	*Ter informatie/geen opmerkingen*
108.	Bij het bepalen van een exitstrategie handelen instellingen en betalingsinstellingen als volgt: a. zij stellen de doelen van de exitstrategie vast; b. zij voeren een bedrijfsimpactanalyse uit in verhouding tot het risico van de uitbestede processen, diensten of activiteiten om na te gaan welke personele en financiële middelen nodig zouden zijn om het exitplan uit te voeren en hoe lang dat zou duren; c. zij wijzen taken, verantwoordelijkheden en voldoende middelen toe voor het beheer van exitplannen en het overbrengen van activiteiten; d. zij stellen criteria op om te bepalen of de overdracht van uitbestede functies en gegevens geslaagd is; en e. zij stellen vast welke indicatoren moeten worden gehanteerd voor de bewaking van de uitbestedingsregeling (zoals beschreven in hoofdstuk 14), met inbegrip van indicatoren die zijn gebaseerd op onaanvaardbare niveaus van dienstverlening die tot een exit moeten leiden.	*Ter informatie/geen opmerkingen*
	Titel V – Richtsnoeren inzake uitbesteding gericht tot bevoegde autoriteiten	
109.	Bij het vaststellen van passende methoden om te controleren of instellingen en betalingsinstellingen aan de voorwaarden voor de oorspronkelijke vergunning voldoen, hebben bevoegde autoriteiten tot doel na te gaan of uitbestedingsregelingen leiden tot een materiële wijziging in de voorwaarden en verplichtingen van de oorspronkelijke vergunning van instellingen en betalingsinstellingen.	*Gericht op toezichthouder.*
110.	Bevoegde autoriteiten vergewissen zich ervan dat zij doeltreffend toezicht op instellingen en betalingsinstellingen kunnen houden, en ook dat instellingen of betalingsinstellingen in hun uitbestedingsregeling hebben vastgelegd dat dienstverleners verplicht zijn om audit- en toegangsrechten aan de bevoegde autoriteit en de instelling toe te kennen, conform 13.3.	*Gericht op toezichthouder.*
111.	De uitbestedingsrisico's van instellingen worden ten minste in het kader van de SREP geanalyseerd, of, als het gaat om betalingsinstellingen, als onderdeel van andere toezichtsprocedures, waaronder ad-hocverzoeken, of tijdens inspecties ter plaatse.	*Gericht op toezichthouder.*

112.	Naar aanleiding van de in het register vastgelegde informatie, als bedoeld in hoofdstuk 11, mogen bevoegde autoriteiten instellingen en betalingsinstellingen om aanvullende informatie verzoeken, met name met het oog op kritieke of belangrijke uitbestedingsregelingen, zoals: a. de gedetailleerde risicoanalyse; b. of de dienstverlener een bedrijfscontinuïteitsplan heeft dat geschikt is voor de aan de uitbestedende instelling of betalingsinstelling te verlenen diensten; c. de te hanteren exitstrategie als een van de partijen de uitbestedingsregeling beëindigt of als er sprake is van verstoring van de dienstverlening; en d. de aanwezige middelen en maatregelen om de uitbestede activiteiten passend te bewaken.	*Gericht op toezichthouder.*
113.	Als aanvulling op de informatie die op grond van hoofdstuk 11 is vereist, kunnen bevoegde autoriteiten van instellingen en betalingsinstellingen gedetailleerde informatie over alle uitbestedingsregelingen verlangen, zelfs als de betrokken functie niet als kritiek of belangrijk wordt beschouwd.	*Gericht op toezichthouder.*
114.	Bevoegde autoriteiten beoordelen het volgende via een op risico's gebaseerde aanpak: a. of instellingen en betalingsinstellingen op passende wijze in het bijzonder kritieke of belangrijke uitbestedingsregelingen bewaken en beheren; b. of instellingen en betalingsinstellingen over voldoende middelen beschikken om uitbestedingsregelingen te bewaken en te beheren; c. of instellingen en betalingsinstellingen alle relevante risico's in kaart brengen en beheren; en d. of instellingen belangenconflicten met betrekking tot uitbestedingsregelingen identificeren, beoordelen en naar behoren beheren, bijvoorbeeld in het geval van uitbesteding binnen de groep of uitbesteding binnen hetzelfde institutionele protectiestelsel.	*Gericht op toezichthouder.*
115.	Bevoegde autoriteiten zorgen ervoor dat EU/EER-instellingen en -betalingsinstellingen niet als "lege huls" opereren, inclusief situaties waarin instellingen van back-to-backtransacties of transacties binnen de groep gebruikmaken om een deel van het marktrisico en kredietrisico aan een niet-EU/EER-entiteit over te dragen, en zien erop toe dat zij passende regelingen voor governance en risicobeheer hebben om hun risico's te identificeren en te beheren.	*Gericht op toezichthouder.*

116.	Tijdens hun beoordeling houden bevoegde autoriteiten rekening met alle risico's, met name: a. de operationele risico's van de uitbestedingsregeling; b. reputatierisico's; c. het instaprisico waardoor de instelling gedwongen kan worden een dienstverlener overeind te houden, als het gaat om belangrijke instellingen; d. concentratierisico's binnen de instelling, inclusief op geconsolideerde basis, veroorzaakt door het bestaan van meerdere uitbestedingsregelingen met één dienstverlener of dienstverleners die nauw met elkaar verbonden zijn, of meerdere uitbestedingsregelingen binnen dezelfde bedrijfssector; e. concentratierisico's op sectorniveau, bijvoorbeeld wanneer meerdere instellingen of betalingsinstellingen gebruikmaken van één dienstverlener of een kleine groep dienstverleners; f. de mate waarin de uitbestedende instelling of betalingsinstelling zeggenschap over de dienstverlener heeft of diens handelingen kan beïnvloeden, de vermindering van risico's die kan voortvloeien uit een grotere mate van zeggenschap en de vraag of de dienstverlener onder het geconsolideerde toezicht van de groep valt; en g. belangenconflicten tussen de instelling en de dienstverlener.	*Gericht op toezichthouder.*
117.	Wanneer concentratierisico's worden geïdentificeerd, volgen bevoegde autoriteiten de ontwikkeling van zulke risico's en beoordelen zij zowel de mogelijke gevolgen voor andere instellingen en betalingsinstellingen als voor de stabiliteit van de financiële markt; bevoegde autoriteiten stellen, waar nodig, de afwikkelingsautoriteit op de hoogte van nieuwe potentieel kritieke functies die zij tijdens de beoordeling in kaart hebben gebracht.	*Gericht op toezichthouder.*
118.	Wanneer wordt vastgesteld dat er punten van zorg zijn waaruit blijkt dat een instelling of betalingsinstelling niet langer solide governanceregelingen heeft of niet aan de regelgevingsvereisten voldoet, nemen bevoegde autoriteiten passende maatregelen, bijvoorbeeld het beperken van de reikwijdte van de uitbestede functies of eisen dat terugtrekking uit een of meer uitbestedingsregelingen plaatsvindt. In het bijzonder kan, aangezien de instelling of betalingsinstelling permanent moet kunnen opereren, de ontbinding van contracten worden verlangd als het toezicht op en de handhaving van de regelgevingsvereisten niet via andere maatregelen kan worden bewerkstelligd.	*Gericht op toezichthouder.*
119.	Bevoegde autoriteiten vergewissen zich ervan dat zij doeltreffend toezicht kunnen uitoefenen, vooral wanneer instellingen en betalingsinstellingen kritieke of belangrijke functies uitbesteden die buiten de EU/EER worden verricht.	*Gericht op toezichthouder.*

Bijlage 2 – ESMA Richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten

	Richtsnoeren	Implementatie bij beleggingsonderneming (*Input Blanco bij uitvoeren analyse)*
	Richtsnoer 1 – Governance, toezicht en documentatie	
12.	Een onderneming moet beschikken over een vastomlijnde en actuele uitbestedingsstrategie voor clouddiensten consistent met de relevante strategieën en interne beleidsmaatregelen en processen van de onderneming, waaronder met betrekking tot informatie- en communicatietechnologie, informatiebeveiliging en operationeel risicobeheer.	*Ter informatie/geen opmerkingen*
13	Een onderneming moet: a) de verantwoordelijkheden voor de documentatie en het beheer van en het toezicht op uitbestedingsovereenkomsten voor clouddiensten binnen haar organisatie duidelijk toekennen; b) voldoende middelen toewijzen om te waarborgen dat aan deze richtsnoeren en alle wettelijke vereisten die voor haar uitbestedingsovereenkomsten voor clouddiensten gelden wordt voldaan; c) een functie voor toezicht op de uitbesteding van clouddiensten in het leven roepen of senior medewerkers aanwijzen die rechtstreeks verantwoording afleggen aan het leidinggevend orgaan en verantwoordelijk zijn voor het beheer van en toezicht op de risico's van uitbestedingsovereenkomsten voor clouddiensten. Bij de naleving van dit richtsnoer moeten ondernemingen rekening houden met de aard, omvang en complexiteit van de onderliggende risico's, ook voor wat betreft het risico voor het financiële systeem en de risico's die verbonden zijn aan de uitbestede functies, en ervoor zorgen dat hun leidinggevend orgaan over de benodigde technische vaardigheden beschikt om de risico's van uitbestedingsovereenkomsten voor clouddiensten te begrijpen. Kleine en minder complexe ondernemingen moeten ten minste zorg dragen voor een duidelijke verdeling van taken en verantwoordelijkheden voor het management van en toezicht op uitbestedingsovereenkomsten voor clouddiensten.	*Ter informatie/geen opmerkingen*
14	Een onderneming moet de uitvoering van functies, de beveiligingsmaatregelen en de naleving van de overeengekomen niveaus van dienstverlening door haar aanbieders van clouddiensten monitoren. Deze monitoring moet risico gebaseerd zijn en vooral gericht zijn op kritieke of belangrijke uitbestede functies.	*Ter informatie/geen opmerkingen*
15	Een onderneming moet periodiek opnieuw beoordelen of haar uitbestedingsovereenkomsten voor clouddiensten een kritieke of belangrijke functie betreffen, en eveneens een dergelijke beoordeling verrichten wanneer een wezenlijke wijziging voordoet in het risico, de aard of de omvang van de uitbestede functie.	*Ter informatie/geen opmerkingen*
16	Een onderneming moet een geactualiseerd register bijhouden met informatie over al haar uitbestedingsovereenkomsten voor clouddiensten en daarbij onderscheid maken tussen de uitbesteding van kritieke of belangrijke functies en niet als kritiek of belangrijk aangemerkte functies. Hierbij moet zij kort aangeven waarom de uitbestede functie al dan niet kritiek of belangrijk wordt geacht. Met	*Ter informatie/geen opmerkingen*

	inachtneming van het nationaal recht moet een onderneming daarnaast gedurende een passende periode een lijst van beëindigde uitbestedingsovereenkomsten voor clouddiensten bijhouden.	
17	Voor de uitbestedingsovereenkomsten voor clouddiensten voor kritieke of belangrijke functies moet het register voor elke uitbestedingsovereenkomst voor clouddiensten ten minste de volgende informatie bevatten: a) een referentienummer; b) de aanvangsdatum en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, de einddatum en/of opzeggingstermijnen voor de CSP en voor de onderneming; c) een korte beschrijving van de uitbestede functie, met inbegrip van de uitbestede gegevens en de vermelding of deze gegevens persoonsgegevens omvatten (bijvoorbeeld door in een afzonderlijk gegevensveld Ja of Nee in te vullen); d) een door de onderneming toegewezen categorie die de aard van de uitbestede functie aangeeft (bijvoorbeeld IT-functie, toezichtfunctie), die het gemakkelijker moet maken om de verschillende soorten uitbestedingsovereenkomsten voor clouddiensten te identificeren; e) vermelding of de uitbestede functie ter ondersteuning dient van tijdgevoelige bedrijfsactiviteiten; f) de naam en de merknaam (indien van toepassing) van de CSP, het land waar deze is geregistreerd, het handelsregisternummer, de identificatiecode voor rechtspersonen (indien van toepassing), het geregistreerde adres, de relevante contactgegevens en de naam van de moederonderneming van het bedrijf (indien van toepassing); g) het toepasselijke recht waardoor de uitbestedingsovereenkomst voor clouddiensten wordt beheerst, en, indien van toepassing, de jurisdictiekeuze; h) het soort clouddiensten en implementatiemodellen en de specifieke aard van de te bewaren gegevens alsook de locaties (te weten landen of regio's) waar die gegevens kunnen worden opgeslagen; i) de datum waarop het kritieke karakter of het belang van de uitbestede functie voor het laatst is beoordeeld en de datum van de volgende geplande beoordeling; j) de datum van de meest recente risicobeoordeling/audit van de CSP alsmede een korte samenvatting van de belangrijkste resultaten, en de datum van de volgende geplande risicobeoordeling/audit; k) de persoon of het besluitvormingsorgaan binnen de onderneming die/dat de uitbestedingsovereenkomst betreffende clouddiensten heeft goedgekeurd; l) indien van toepassing, de namen van onderaannemers waaraan kritieke of belangrijke onderdelen (of wezenlijke onderdelen daarvan) zijn onderuitbesteed, inclusief de landen waar de onderaannemers zijn geregistreerd, waar de onderuitbestede dienst zal worden verricht en de locatie (te weten landen of regio's) waar de gegevens zullen worden opgeslagen; m) de geraamde jaarlijkse begrotingskosten van de uitbestedingsovereenkomst voor clouddiensten.	*Zie tevens hoofdstuk 4.7 van de Blanco-paper*
18	Voor de uitbestedingsovereenkomsten voor clouddiensten voor niet-kritieke of niet- belangrijke functies moet een onderneming op basis van de aard, de omvang en complexiteit van de aan de uitbestede functie verbonden risico's bepalen welke gegevens in het register worden opgenomen.	*Zie tevens paragraaf 4.2 en 4.3 van de Blanco-paper*
	Richtsnoer 2 – Analyse voorafgaand aan uitbesteding en due diligence	

19	Voordat een onderneming een uitbestedingsovereenkomst voor clouddiensten aangaat, moet zij: a) beoordelen of de uitbestedingsovereenkomst voor clouddiensten betrekking heeft op een kritieke of belangrijke functie; b) alle relevante risico's van de uitbestedingsovereenkomst betreffende clouddiensten vaststellen en beoordelen; c) een passend due diligence-onderzoek uitvoeren ten aanzien van de potentiele CSP; d) mogelijke belangenconflicten als gevolg van de uitbesteding identificeren en beoordelen.	*Zie tevens paragraaf 2.1, 4.2 en 4.3 van de Blanco-paper*
20	De voorafgaand aan uitbesteding verrichte analyse en het due diligence-onderzoek ten aanzien van de potentiële CSP moeten in verhouding staan tot de aard, de omvang en complexiteit van de functie die de onderneming wil uitbesteden en de risico's die met deze functie verbonden zijn. Er moet in elk geval een beoordeling worden uitgevoerd van de mogelijke gevolgen van de uitbestedingsovereenkomst voor clouddiensten voor de operationele, juridische, nalevings- en reputatierisico's voor de onderneming.	*Zie tevens paragraaf 4.2 van de Blanco-paper*
21	Ingeval de uitbestedingsovereenkomst voor clouddiensten kritieke of belangrijke functies betreft, moet een onderneming ook: a) een beoordeling maken van alle relevante risico's die kunnen voortvloeien uit de uitbestedingsovereenkomst voor clouddiensten, waaronder risico's met betrekking tot informatie- en communicatietechnologie, informatiebeveiliging, bedrijfscontinuïteit, juridische, nalevings-, reputatie- en operationele risico's, alsmede mogelijke toezichtsbelemmeringen voor de onderneming die het gevolg zijn van: i. de geselecteerde clouddienst en de voorgestelde implementatiemodellen; ii. het migratie- en/of uitvoeringsproces; iii. de gevoeligheid van de functie en de betrokken gegevens die het bedrijf eventueel wil uitbesteden en de beveiligingsmaatregelen die zouden moeten worden genomen; iv. de interoperabiliteit van de systemen en applicaties van de onderneming en van de CSP, dat wil zeggen hun vermogen om informatie uit te wisselen en deze uitgewisselde informatie te gebruiken; v. de overdraagbaarheid van de gegevens van de onderneming, te weten de mogelijkheid om de ondernemingsgegevens eenvoudig van de ene CSP over te dragen aan een andere aanbieder of aan de onderneming zelf; vi. de politieke stabiliteit, de veiligheidssituatie en het rechtssysteem (met inbegrip van de geldende rechtshandhavingsbepalingen, de bepalingen uit het insolventierecht die van toepassing zouden zijn in geval van faillissement van de CSP , de geldende regelgeving inzake gegevensbescherming en de vraag of er is voldaan aan de voorwaarden voor de overdracht van persoonsgegevens aan een derde land overeenkomstig de AVG) van de landen (binnen of buiten de EU) waar de uitbestede functies zouden worden verricht en waar de uitbestede gegevens zouden worden opgeslagen; in het geval van onderuitbesteding, de aanvullende risico's die kunnen ontstaan als de onderaannemer zich in een derde land of in een ander land dan de CSP bevindt en, in het geval van een onderuitbestedingsketen, elk aanvullend risico dat zich kan voordoen, ook door het ontbreken van een directe overeenkomst tussen de onderneming en de onderaannemer die de uitbestede functie verricht;	*Op verzoek stelt Blanco graag nadere informatie ter beschikking ten aanzien van de informatie- en communicatietechnologie, de informatiebeveiliging en de continuïteit. Uiteraard is het aan de onderneming zelf om de risico's in kaart te brengen en eventuele maatregelen te treffen.* *Zie tevens paragraaf 4.2. van de Blanco-paper*

	vii. een mogelijke concentratie binnen de onderneming (waar van toepassing tevens op het niveau van de groep waarvan de onderneming deel uitmaakt) die wordt veroorzaakt doordat met één en dezelfde CSP meerdere uitbestedingsovereenkomsten voor clouddiensten zijn aangegaan, en een mogelijke concentratie binnen de financiële sector in de EU doordat meerdere ondernemingen gebruikmaken van dezelfde CSP of een kleine groep van aanbieders van clouddiensten. Bij de beoordeling van het concentratierisico moet de onderneming al haar uitbestedingsovereenkomsten voor clouddiensten met die CSP in aanmerking nemen (en, waar van toepassing, de uitbestedingsovereenkomsten voor clouddiensten op het niveau van de groep waarvan zij deel uitmaakt); b) rekening houden met de verwachte voordelen en kosten van de uitbestedingsovereenkomst betreffende clouddiensten, met inbegrip van een afweging tussen de significante risico's die kunnen worden verkleind of beter kunnen worden beheerd, en eventuele significante risico's die zich kunnen voordoen als gevolg van de uitbestedingsovereenkomst betreffende clouddiensten.	
22	In geval van uitbesteding van kritieke of belangrijke functies moet een evaluatie van de geschiktheid van de CSP deel uitmaken van het due diligence-onderzoek. Bij de beoordeling van de geschiktheid van de CSP moet een onderneming ervoor zorgen dat de CSP over de bedrijfsreputatie, de vaardigheden, de middelen (waaronder personele, IT- en financiële middelen), de organisatiestructuur en, indien van toepassing, de benodigde vergunning(en) of registratie(s) beschikt om de kritieke of belangrijke functie op betrouwbare en professionele wijze te verrichten en zijn verplichtingen gedurende de looptijd van de uitbestedingsovereenkomst voor clouddiensten na te komen. Aanvullende factoren die in een due diligence-onderzoek naar de CSP moeten worden onderzocht, zijn onder meer: a) het beheer van informatiebeveiliging en met name de bescherming van persoonsgegevens en vertrouwelijke of anderszins gevoelige gegevens; b) de door de CSP geboden support, met inbegrip van supportplannen en contactpersonen voor support, en procedures op het gebied van incidentenbeheer; c) de plannen inzake bedrijfscontinuïteit en rampenherstel.	*Op verzoek stelt Blanco graag nadere informatie ter beschikking ten aanzien van de informatie- en communicatietechnologie, de informatiebeveiliging en de continuïteit. Een SLA maakt standaard onderdeel uit van de overeenkomst met Blanco.* *Zie tevens paragraaf 4.2. van de Blanco-paper*
23	Waar van toepassing en om het uitgevoerde due diligence-onderzoek te ondersteunen, kan een onderneming tevens gebruikmaken van certificeringen op basis van internationale normen en verslagen van externe of interne audits.	*Blanco beschikt over een ISAE3402 Type 2 certificering.*
24	Als een onderneming aanzienlijke tekortkomingen en/of veranderingen in de verrichte diensten of de situatie van de CSP vaststelt, moeten de voorafgaand aan uitbesteding verrichte analyse en het due diligence-onderzoek ten aanzien van de aanbieder onmiddellijk worden herzien of waar nodig opnieuw worden uitgevoerd.	*Ter informatie/geen opmerkingen*
25	Indien een onderneming een nieuwe overeenkomst sluit met een reeds beoordeelde CSP of een bestaande overeenkomst verlengt, moet zij middels een op risico gebaseerde benadering vaststellen of er een nieuw due diligence-onderzoek nodig is.	*Ter informatie/geen opmerkingen*
	Richtsnoer 3 – Essentiële contractuele bepalingen	
26	De respectievelijke rechten en plichten van een onderneming en haar CSP moeten duidelijk in een schriftelijke overeenkomst worden vastgelegd.	*Blanco sluit met alle cliënten een schriftelijke overeenkomst.*

27	De schriftelijke overeenkomst moet de onderneming uitdrukkelijk de mogelijkheid bieden om de overeenkomst indien nodig te beëindigen.	*De overeenkomst met Blanco bevat een uitgebreide 'looptijd en beëindigingsclausule'. In beginsel heeft de overeenkomst een bepaalde duur, maar is het mogelijk onder omstandigheden de overeenkomst voortijdig te beëindigen.*
28	In geval van uitbesteding van kritieke of belangrijke functies moet de schriftelijke overeenkomst minimaal het volgende bevatten: a) een heldere beschrijving van de uitbestede functie; b) de aanvangsdatum en de einddatum van de overeenkomst, indien van toepassing, en de opzegtermijnen voor de CSP en de onderneming; c) het toepasselijke recht dat op de overeenkomst van toepassing is, en, indien van toepassing, de jurisdictiekeuze; d) de financiële verplichtingen van de onderneming en van de CSP; e) vermelding of onderuitbesteding is toegestaan en zo ja, onder welke voorwaarden, gelet op richtsnoer 7; f) de locatie(s) (te weten landen of regio's) waar de uitbestede functie zal worden verricht en gegevens zullen worden verwerkt en opgeslagen, en de voorwaarden waaraan moet worden voldaan, met inbegrip van een verplichting om de onderneming in kennis te stellen als de CSP voorstelt de locatie(s) te wijzigen; g) de bepalingen inzake informatiebeveiliging en de bescherming van persoonsgegevens, gelet op richtsnoer 4; h) het recht voor de onderneming om de prestaties van de CSP uit hoofde van de uitbestedingsovereenkomst voor clouddiensten regelmatig te monitoren, gelet op richtsnoer 6; i) de overeengekomen niveaus van dienstverlening, die kwantitatieve en kwalitatieve prestatiedoelen moeten omvatten om tijdige controle mogelijk te maken, zodat zonder onnodig uitstel passende corrigerende beheersmaatregelen kunnen worden genomen indien de overeengekomen dienstverleningsniveaus niet worden gehaald; j) de verplichtingen van de CSP tot verslaglegging aan de onderneming, en, indien nodig, de verplichtingen om verslagen in te dienen die relevant zijn voor de veiligheidsfunctie en cruciale functies van de onderneming, zoals verslagen van de interne-auditfunctie van de CSP; k) de bepalingen inzake het incidentenbeheer door de CSP, met inbegrip van de verplichting voor de CSP om de onderneming zonder onnodig uitstel op de hoogte te stellen van incidenten die de uitvoering van de uitbestede dienst van de onderneming hebben beïnvloed; l) vermelding of de CSP zich verplicht tegen bepaalde risico's dient te verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking; m) de verplichting van de CSP om de plannen voor bedrijfscontinuïteit en rampenherstel in te voeren en te testen; n) de verplichting van de CSP om de onderneming, de betreffende bevoegde autoriteiten en elke andere door de onderneming of de bevoegde autoriteiten aangewezen persoon toegangsrechten en voor de relevante informatie, locaties, systemen en apparaten van de CSP inspectierechten (onderzoeks- en"auditrechten") toe te kennen voor zover deze nodig zijn om de prestaties van de CSP uit hoofde van de uitbestedingsovereenkomst voor clouddiensten en zijn naleving van de geldende wettelijke voorschriften en contractuele vereisten te monitoren, gelet op richtsnoer 6; o) bepalingen om te waarborgen dat de gegevens die de CSP namens de onderneming verwerkt of opslaat, waar nodig toegankelijk zijn en kunnen worden hersteld en geretourneerd aan de onderneming, gelet op richtsnoer 5.	*Alle genoemde onderwerpen zijn opgenomen in de standaard overeenkomst met Blanco.* *Zie tevens paragraaf 4.4. van de Blanco-paper.*

	Richtsnoer 4 - Informatiebeveiliging	
29	Een onderneming moet informatiebeveiligingseisen opnemen in haar interne beleid en procedures en in de schriftelijke uitbestedingsovereenkomst voor clouddiensten en de naleving van deze eisen voortdurend monitoren, mede om vertrouwelijke, persoons- of anderszins gevoelige gegevens te beschermen. Deze eisen moeten in verhouding staan tot de aard, schaal en complexiteit van de functie die de onderneming uitbesteedt aan de CSP en de risico's die met deze functie verbonden zijn.	*Ter informatie/geen opmerkingen*
30	Daarvoor moet een onderneming in geval van uitbesteding van kritieke of belangrijke functies, en zonder afbreuk te doen aan de toepasselijke eisen uit de AVG, middels een op risico gebaseerde benadering ten minste: a) organisatie voor informatiebeveiliging: waarborgen dat informatiebeveiligingsrollen en -verantwoordelijkheden duidelijk zijn verdeeld tussen de onderneming en de CSP , ook met betrekking tot detectie van bedreigingen, incidenten- en patchbeheer, en dat de CSP zijn rollen en verantwoordelijkheden daadwerkelijk kan vervullen en na kan komen; b) identiteits- en toegangsbeheer: ervoor zorgen dat er sterke authenticatiemechanismen (bijvoorbeeld tweefactorauthenticatie) en toegangsmaatregelen zijn geïmplementeerd om ongeoorloofde toegang tot de gegevens en back-end cloudresources van de onderneming te voorkomen; c) versleuteling en sleutelbeheer: ervoor zorgen dat er waar nodig gebruik wordt gemaakt van relevante versleutelingstechnologieën voor gegevens in transit, opgeslagen gegevens, gegevens in rusttoestand en gegevensback-ups in combinatie met passende sleutelbeheeroplossingen om het risico van ongeoorloofde toegang tot versleutelingscodes te beperken; met name bij de keuze van een sleutelbeheeroplossing moet de onderneming aandacht besteden aan geavanceerde technologie en processen ; d) operationele en netwerkbeveiliging: aandacht besteden aan passende niveaus van beschikbaarheid en scheiding van netwerken (bijvoorbeeld tenantisolatie in de gedeelde cloudomgeving, operationele scheiding van web, applicatielogica, besturingssysteem, netwerk, database management systeem (DBMS) en opslaglagen) en verwerkingsomgevingen (bijvoorbeeld test-, gebruikersacceptatietest-, ontwikkel- en productieomgeving); e) application programming interfaces (API's): aandacht besteden aan mechanismen voor de integratie van de clouddiensten met de systemen van de onderneming om de veiligheid van API's te waarborgen (bijvoorbeeld door voor meerdere systeeminterfaces, jurisdicties en bedrijfsfuncties informatiebeveiligingsbeleid en - procedures voor API's op te zetten en te onderhouden om ongeoorloofde openbaarmaking, wijziging of vernietiging van gegevens te voorkomen); f) bedrijfscontinuïteit en rampenherstel: zorgen voor doeltreffende beheersmaatregelen ten aanzien van bedrijfscontinuïteit en rampenherstel (bijvoorbeeld door minimumcapaciteitsvereisten vast te stellen, geografisch gespreide hostingopties te selecteren waarbij tussen de verschillende opties kan worden gewisseld, of door documentatie op te vragen en door te nemen die laat zien welke route de gegevens van de onderneming tussen de systemen van de CSP volgen, alsmede door de mogelijkheid te overwegen om machine images naar een onafhankelijke opslaglocatie te kopiëren die voldoende geïsoleerd is van het netwerk of offline is); g) gegevenslocatie: een op risico gebaseerde benadering volgen ten aanzien van gegevensopslag- en gegevensverwerkingslocatie(s) (te weten landen of regio's); h) naleving en monitoring: verifiëren dat de CSP voldoet aan internationaal erkende informatiebeveiligingsnormen en passende informatiebeveiligingsmaatregelen heeft	*In de overeenkomst staan de minimale informatiebeveiligingsmaatregelen genoemd. Naast deze algemene maatregelen treft Blanco nadere maatregelen, afhankelijk van de module en/of suite die van Blanco wordt afgenomen. Op verzoek kan Blanco nadere toelichting verschaffen.* *Blanco heeft een informatiebeveiligingsbeleid wat in scope is van de ISAE3402 van Blanco.*

	geïmplementeerd (bijvoorbeeld door de CSP te vragen aan te tonen dat hij relevante informatiebeveiligingsmaatregelen uitvoert en de informatiebeveiligingsmaatregelen van de CSP regelmatig beoordeelt en test).	
	Richtsnoer 5 - Exitstrategieën	
31	In geval van uitbesteding van kritieke of belangrijke functies moet een onderneming ervoor zorgen dat zij de uitbestedingsovereenkomst voor clouddiensten kan beëindigen zonder onnodige verstoring van haar bedrijfsactiviteiten en dienstverlening aan klanten en zonder dat de naleving van haar verplichtingen uit hoofde van de toepasselijke wetgeving en de vertrouwelijkheid, integriteit en beschikbaarheid van haar gegevens enig nadeel ondervinden. Daarvoor moet een onderneming: a) exitplannen ontwikkelen en implementeren die volledig, gedocumenteerd en voldoende getest zijn. Deze plannen moeten waar nodig worden geactualiseerd, onder meer in geval van wijzigingen in de uitbestede functie; b) met alternatieve oplossingen komen en overgangsplannen ontwikkelen om de uitbestede functie en gegevens bij de CSP en, indien van toepassing, bij eventuele onderaannemers weg te halen en over te dragen aan de andere CSP, zoals aangegeven door de onderneming, of rechtstreeks aan de onderneming zelf. Deze oplossingen moeten worden vastgesteld met het oog op de uitdagingen die zich kunnen voordoen door de locatie van de gegevens, en daarbij moeten de nodige beheersmaatregelen worden genomen om de bedrijfscontinuïteit tijdens de overgangsfase te waarborgen; c) ervoor zorgen dat de schriftelijke uitbestedingsovereenkomst voor de CSP de verplichting omvat om de uitbestede functie en de daarmee samenhangende verwerking van gegevens ordentelijk over te dragen van de CSP en eventuele onderaannemers aan een andere CSP, zoals aangegeven door de onderneming, of rechtstreeks aan de onderneming zelf ingeval de onderneming de exitstrategie in werking stelt. De verplichting om de ordentelijke overdracht van de uitbestede functie en de daarmee samenhangende verwerking van gegevens te ondersteunen moet waar relevant ook de veilige verwijdering van de gegevens uit de systemen van de CSP en eventuele onderaannemers omvatten.	*Blanco heeft in de overeenkomst een 'exit assistentie' beding opgenomen. Daarnaast zijn er in de overeenkomst bepalingen opgenomen ten aanzien van de overdracht en/of verwijdering van (persoons)gegevens.*
32	Bij de ontwikkeling van de exitplannen en oplossingen waarnaar wordt verwezen in de bovenstaande punten a) en b) ("exitstrategie") moet de onderneming aandacht besteden aan: a) de vaststelling van de doelen van de exitstrategie; b) de aanwijzing van gebeurtenissen waarbij de exitstrategie in werking kan worden gesteld. Hiertoe moeten in elk geval de beëindiging van de uitbestedingsovereenkomst voor clouddiensten op initiatief van de onderneming of de CSP en het faillissement of een andere ernstige onderbreking van de bedrijfsactiviteiten van de CSP worden gerekend; c) de uitvoering van een effectbeoordeling van de potentiële bedrijfsschade die in verhouding staat tot de uitbestede functie om na te gaan welke personele en andere middelen er nodig zouden zijn om de exitstrategie uit te voeren; d) de toewijzing van rollen en verantwoordelijkheden voor het beheer van de exitstrategie; e) de toetsing van de geschiktheid van de exitstrategie te testen middels een op risico gebaseerde benadering (bijvoorbeeld door middel van een analyse van de potentiële kosten, gevolgen, middelen en implicaties voor de tijdsplanning van de overdracht van een uitbestede dienst aan een andere aanbieder); f) de opstelling van criteria om te bepalen of de overgang is geslaagd.	*Ter informatie/geen opmerkingen*

33	Een onderneming moet indicatoren van de gebeurtenissen waarbij de exitstrategie in werking kan worden gesteld opnemen in haar doorlopende monitoring van en toezicht op de diensten die de CSP uit hoofde van de uitbestedingsovereenkomst voor clouddiensten verricht.	*Ter informatie/geen opmerkingen*
34	Een onderneming moet ervoor zorgen dat de schriftelijke uitbestedingsovereenkomst voor clouddiensten geen beperkingen oplegt aan de doeltreffende uitoefening van het toegangs- en auditrecht en toezichtopties ten aanzien van de CSP door de onderneming en de bevoegde autoriteit.	*De standaard overeenkomst bevat een right to audit en right to examine.*
35	Een onderneming moet ervoor zorgen dat bij de uitoefening van het toegangs- en auditrecht (zoals de auditfrequentie en de te controleren gebieden en diensten) rekening wordt gehouden met de vraag of de uitbesteding verband houdt met een kritieke of belangrijke functie en met de aard en omvang van de risico's en gevolgen van de uitbestedingsovereenkomst voor clouddiensten voor de onderneming.	*Ter informatie/geen opmerkingen*
36	Ingeval de uitoefening van het toegangs- of auditrecht of het gebruik van bepaalde audittechnieken een risico oplevert voor de omgeving van de CSP en/of een andere klant van de CSP (bijvoorbeeld doordat deze/dit gevolgen heeft voor de dienstverleningsniveaus of de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens), moet de CSP duidelijk aangeven waarom dit een risico zou opleveren en samen met de onderneming alternatieve werkwijzen overeenkomen om een vergelijkbaar resultaat te bereiken (bijvoorbeeld de opname van specifieke beheersmaatregelen die worden getest in een specifiek verslag/specifieke certificering van de CSP).	*Ter informatie/geen opmerkingen. Een audit zal altijd in overleg worden uitgevoerd, waarbij de rechten en plichten van zowel de onderneming als van Blanco en andere klanten van Blanco in acht worden genomen.*
37	Onverminderd hun eindverantwoordelijkheid ten aanzien van uitbestedingsovereenkomsten voor clouddiensten kunnen ondernemingen, om hun auditmiddelen efficiënter aan te wenden en de organisatorische lasten voor de CSP en zijn klanten te verlichten, gebruikmaken van: a) door de CSP verstrekte externe certificeringen en externe of interne auditrapportages; b) gemeenschappelijke audits die samen met andere klanten van dezelfde CSP of door een door meerdere klanten van dezelfde CSP aangestelde externe auditor worden uitgevoerd.	*Blanco heeft ISAE3402 Type 2*
38	In geval van uitbesteding van kritieke of belangrijke functies moet een onderneming beoordelen of de in punt 37, onder a), bedoelde externe certificeringen en externe of interne auditverslagen passend en toereikend zijn om aan haar verplichtingen uit hoofde van de toepasselijke wetgeving te voldoen, en moet zij ernaar streven na verloop van tijd niet uitsluitend gebruik te maken van deze certificeringen en verslagen.	*Ter informatie/geen opmerkingen*
39	In geval van uitbesteding van kritieke of belangrijke functies mag een onderneming alleen gebruikmaken van de in punt 37, onder a), bedoelde externe certificeringen en externe of interne auditverslagen als zij: a) erop toeziet dat de certificeringen of auditverslagen betrekking hebben op de essentiële systemen van de CSP (bijvoorbeeld processen, applicaties, infrastructuur, gegevenscentra), de door de onderneming vastgestelde essentiële beheersmaatregelen en de naleving van de relevante toepasselijke wetgeving; b) de inhoud van de certificeringen of auditverslagen regelmatig grondig beoordeelt en nagaat of de certificeringen of verslagen niet verouderd zijn; c) erop toeziet dat ook toekomstige versies van de certificeringen of auditverslagen betrekking hebben op essentiële systemen en beheersmaatregelen van de CSP; d) zich heeft vergewist van de geschiktheid van de certificerende of controlerende partij (bijvoorbeeld met betrekking tot de kwalificaties, deskundigheid, herhaling van de uitvoering/controle van bewijsstukken in het betrokken auditdossier en de roulering van de certificerende of controlerende organisatie); e) zich ervan heeft vergewist dat de certificeringen zijn afgegeven, dat de audits zijn uitgevoerd overeenkomstig passende normen en dat deze een toetsing omvatten van de doeltreffendheid van de aanwezige essentiële beheersmaatregelen;	*Op dit moment beschikt Blanco over twee ISAE3402 rapporten;; een ten aanzien van de KYC Suite en een ten aanzien van het PMS. De scope van de ISAE3402 ten aanzien van de KYC Suite heeft betrekking op informatiebeveiliging, privacy en ontwikkelprocessen. Een groot deel van deze processen zijn overigens generiek voor heel Blanco. De ISAE3402 die betrekking heeft op PMS heeft met name dataverwerking in scope.* *Blanco werkt toe naar een situatie waarin beide suites gedekt worden door 1 ISAE3402 (verwacht 2022).* *De rapporten worden jaarlijks door een onafhankelijke auditor afgegeven.*

	f) contractueel gerechtigd is te verzoeken om uitbreiding van de reikwijdte van de certificeringen of auditverslagen tot andere relevante systemen en beheersmaatregelen van de CSP, waarbij geldt dat het aantal en de frequentie van dergelijke verzoeken redelijk en vanuit het oogpunt van risicobeheer gerechtvaardigd moeten zijn; g) het contractuele recht behoudt om naar eigen inzicht individuele audits op locatie uit te voeren ten aanzien van de uitbestede functie.	
40	Een onderneming moet de CSP voorafgaand aan een locatiebezoek – ook van een derde door de onderneming aangewezen partij (bijvoorbeeld een auditor) – hiervan binnen een redelijke termijn vooraf in kennis stellen, tenzij een voorafgaande kennisgeving niet mogelijk is vanwege een noodgeval of crisissituatie of tot een situatie zou leiden waarin de audit niet langer doeltreffend zou zijn. In deze kennisgeving moeten de locatie en het doel van het bezoek worden vermeld, evenals het personeel dat aan het bezoek zal deelnemen	*De standaard overeenkomst bevat een right to audit en right to examine.*
41	Aangezien clouddiensten technisch bijzonder complex zijn en specifieke uitdagingen op het gebied van bevoegdheid met zich meebrengen, moet het personeel dat de audit verricht – de interne auditors van de onderneming of de namens haar handelende auditors – over de juiste vaardigheden en kennis beschikken om de betreffende clouddiensten te beoordelen en een doeltreffende en relevante audit te verrichten. Hetzelfde moet gelden voor het personeel van de onderneming dat de certificeringen of auditverslagen van de CSP evalueert.	*Ter informatie/geen opmerkingen*
	Richtsnoer 7 - Onderuitbesteding	
42	Indien onderuitbesteding van kritieke of belangrijke functies (of wezenlijke onderdelen daarvan) is toegestaan, moet(en) in de schriftelijke uitbestedingsovereenkomst voor clouddiensten tussen de onderneming en de CSP: a) elk deel of aspect van de uitbestede functie worden aangegeven dat van potentiële onderuitbesteding is uitgesloten; b) de voorwaarden worden vermeld waaraan in het geval van onderuitbesteding moet worden voldaan. c) worden aangegeven dat de CSP aansprakelijk blijft en de onderuitbestede diensten moet monitoren en controleren, om te waarborgen dat alle contractuele verplichtingen tussen hem en de onderneming voortdurend worden nagekomen; d) een verplichting worden opgenomen voor de CSP om de onderneming in kennis te stellen van elke beoogde onderuitbesteding of wezenlijke wijzigingen daarvan, met name waar deze gevolgen kan hebben voor het vermogen van de CSP om aan zijn verplichtingen uit hoofde van de uitbestedingsovereenkomst voor clouddiensten met de onderneming te voldoen. De in de schriftelijke overeenkomst vastgelegde kennisgevingstermijn moet de onderneming voldoende tijd bieden om ten minste een risicobeoordeling van de voorgestelde onderuitbesteding of wezenlijke wijzigingen daarvan uit te voeren en hiertegen bezwaar te maken dan wel deze uitdrukkelijk goed te keuren, zoals hieronder aangegeven in punt e); e) worden gewaarborgd dat de onderneming het recht heeft bezwaar te maken tegen de beoogde onderuitbesteding of wezenlijke wijzigingen daarvan, of dat expliciete goedkeuring nodig is voordat de voorgestelde onderuitbesteding of wezenlijke wijzigingen van kracht worden; f) worden gewaarborgd dat de onderneming contractueel gerechtigd is de uitbestedingsovereenkomst voor clouddiensten met de CSP te beëindigen ingeval zij bezwaar maakt tegen de voorgestelde onderuitbesteding of wezenlijke wijzigingen daarvan en in geval van onrechtmatige onderuitbesteding (bijvoorbeeld wanneer de CSP overgaat tot	*De standaard overeenkomst van Blanco maakt het mogelijk om diensten onder uit te besteden. Vooral in de KYC Suite maakt Blanco gebruik van dienstverleners die gespecialiseerd zijn in een deel van de dienst, bijvoorbeeld digitaal ondertekenen, het screenen op sanctie- en PEPlijsten of adverse media, en het online verifiëren van de identiteit van klanten.* *Klanten kunnen bezwaar maken tegen onderuitbesteding en kunnen besluiten bepaalde functionaliteiten (waarvoor van onderuitbesteding gebruik wordt gemaakt) niet te gebruiken. Mogelijk kan het bezwaar tegen bepaalde onderuitbestedingen leiden tot het beëindigen van de overeenkomst, bijvoorbeeld als Blanco redelijkerwijs niet tegemoet kan komen aan het bezwaar.*

	onderuitbesteding zonder de onderneming hiervan in kennis te stellen of de voorwaarden van de onderuitbesteding zoals vermeld in de uitbestedingsovereenkomst ernstig schendt).	
43	De onderneming dient ervoor te zorgen dat de CSP adequaat toezicht houdt over de onderaannemer.	*Alvorens over te gaan tot onderuitbesteding, zal Blanco altijd onderzoek doen naar de betreffende dienstverlener en deze ook gedurende de dienstverlening blijven monitoren.*
	Richtsnoer 8 – Schriftelijke kennisgeving aan bevoegde autoriteiten	
44	De onderneming moet de bevoegde autoriteit tijdig schriftelijk in kennis stellen van geplande uitbestedingsovereenkomsten voor clouddiensten die een kritieke of belangrijke functie betreffen. Daarnaast moet de onderneming de bevoegde autoriteit tijdig schriftelijk in kennis stellen van die uitbestedingsovereenkomsten voor clouddiensten die een functie betreffen die eerder als niet-kritiek of niet-belangrijk werd aangemerkt en vervolgens kritiek of belangrijk werd.	*Zie tevens paragraaf 4.5. van de Blanco-paper.*
45	De schriftelijke kennisgeving van de onderneming moet, met inachtneming van het evenredigheidsbeginsel, ten minste de volgende informatie bevatten: a) de aanvangsdatum van de uitbestedingsovereenkomst voor clouddiensten en, indien van toepassing, de eerstvolgende datum van de verlenging van het contract, en de einddatum en/of opzeggingstermijnen voor de CSP en voor de onderneming; b) een korte beschrijving van de uitbestede functie; c) een korte samenvatting van de redenen waarom de uitbestede functie kritiek of belangrijk wordt geacht; d) de naam en de merknaam (indien van toepassing) van de CSP, het land waar deze is geregistreerd, het handelsregisternummer, de identificatiecode voor rechtspersonen (indien van toepassing), het geregistreerde adres, de relevante contactgegevens en de naam van de moederonderneming van het bedrijf (indien van toepassing); e) het toepasselijke recht waardoor de uitbestedingsovereenkomst voor clouddiensten wordt beheerst, en, indien van toepassing, de jurisdictiekeuze; f) de implementatiemodellen voor clouddiensten en de specifieke aard van de door de CSP te bewaren gegevens en de locaties (te weten landen of regio's) waar die gegevens zullen worden opgeslagen; g) de datum waarop het kritieke karakter of het belang van de uitbestede functie voor het laatst is beoordeeld; h) de datum van de meest recente risicobeoordeling of audit van de CSP alsmede een korte samenvatting van de belangrijkste resultaten, en de datum van de volgende geplande risicobeoordeling of audit; i) de persoon of het besluitvormingsorgaan binnen de onderneming die/dat de uitbestedingsovereenkomst betreffende clouddiensten heeft goedgekeurd; j) indien van toepassing, de namen van de onderaannemer waaraan wezenlijke onderdelen van een kritieke of belangrijke functie zijn onderuitbesteed, inclusief het land of de regio waar de onderaannemers zijn geregistreerd, waar de onderuitbestede dienst zal worden verricht en waar de gegevens zullen worden opgeslagen.	*Zie tevens paragraaf 4.5. van de Blanco-paper. Voor meldingen aan de AFM moet gebruik worden gemaakt van een voorgeschreven meldingsformulier.*
	Richtsnoer 9 – Toezicht op uitbestedingsovereenkomsten voor clouddiensten	
46	Als onderdeel van hun toezichtproces moeten bevoegde autoriteiten de risico's die voortvloeien uit door de onderneming gesloten uitbestedingsovereenkomsten betreffende clouddiensten beoordelen. Deze	*Gericht op toezichthouder.*

	beoordeling moet vooral zijn gericht op de overeenkomsten die betrekking hebben op de uitbesteding van kritieke of belangrijke functies.	
47	Bevoegde autoriteiten vergewissen zich ervan dat zij doeltreffend toezicht kunnen uitoefenen, vooral wanneer ondernemingen kritieke of belangrijke functies uitbesteden die buiten de EU worden verricht	*Gericht op toezichthouder.*
48	Bevoegde autoriteiten moeten op basis van een risicogebaseerde aanpak beoordelen of ondernemingen: a) beschikken over de nodige governance, middelen en operationele processen om waar nodig en doeltreffend uitbestedingsovereenkomsten betreffende clouddiensten te sluiten, uit te voeren en hierop toezicht te houden; b) alle relevante risico's in verband met de uitbesteding betreffende clouddiensten identificeren en beheren.	*Gericht op toezichthouder.*
49	Wanneer concentratierisico's worden vastgesteld, moeten bevoegde autoriteiten de ontwikkeling van deze risico's monitoren en de mogelijke gevolgen hiervan voor andere ondernemingen waarop zij toezicht uitoefenen en voor de stabiliteit van de financiële markt evalueren.	*Gericht op toezichthouder.*

Bijlage 3 – DNB Risicoanalyse template uitbesteding

Nr.	Onderwerp	Toelichting	Analyse	Kans	Impact	Risico	Maatregelen	Restrisico
1	Vendor lock-in	Het risico dat niet of niet eenvoudig naar een andere dienstverlener kan worden overgestapt, bijvoorbeeld doordat zich technische beperkingen voordoen, er te weinig andere dienstverleners zijn of de huidige dienstverlener geen ondersteuning kan of wil verlenen bij de overstap naar een concurrent.					Input Blanco: • Blanco wil er zoveel mogelijk voor zorgen dat data van klanten makkelijk te transporteren is en heeft een open architectuur zodat de software van Blanco makkelijk kan samenwerken met andere software die klanten gebruiken • De dienstverlenings-overeenkomst met Blanco kan contractueel relatief makkelijk worden opgezegd • In geval van een faillissement van Blanco is er contractueel een continuïteitsmaatregel overeengekomen, waarbij een Stichting tijdelijk de dienstverlening van Blanco overneemt, zodat de beleggingsonderneming een andere leverancier kan selecteren of kan besluiten de diensten zelf uit te voeren. • De beleggingsonderneming kan een lijst bijhouden van potentiële partijen die (delen van) de dienstverlening van Blanco kunnen overnemen indien noodzakelijk.	

2	Er zijn te weinig middelen om acquisities en/of bestaande uitbestedingsovereen komsten te managen.	De instelling heeft middelen (d.w.z. kennis en personeel) nodig voor de acquisitie, voor de toepassing van uitbestedingsoplossingen en voor de monitoring van leveranciers. Bij dit laatste gaat het om de prestaties van de dienstverlener, maar ook om de interne beheersing, de beheersing van IT-risico's en de beveiliging. Door een tekort aan middelen wordt de uitbesteding niet (langer) gemanaged, waardoor de instelling ongewenste risico's kan lopen, die niet worden gesignaleerd of aangepakt.	.				Input Blanco: • Blanco kan de beleggingsonderneming periodiek haar ISAE3402 rapport verstrekken, waarbij een externe auditor een oordeel velt over de IT-omgeving van Blanco. • De overeenkomst met Blanco bevat verplichte clausules, bijvoorbeeld ten aanzien van audit.	
3	Concentratie	Als één dienstverlener meerdere uitbestedingsoplossingen levert, kan de totale impact van eventuele uitval steeds verder toenemen bij iedere activiteit die de dienstverlener nog meer aan de instelling levert.					Input Blanco: • Blanco wil er zoveel mogelijk voor zorgen dat data van klanten makkelijk te transporteren is en heeft een open architectuur zodat de software van Blanco makkelijk kan samenwerken met andere software die klanten gebruiken • De dienstverlenings-overeenkomst met Blanco kan contractueel relatief makkelijk worden opgezegd, indien nodig • In geval van een faillissement van Blanco is er contractueel een continuïteitsmaatregel overeengekomen, waarbij een Stichting tijdelijk de dienstverlening van Blanco overneemt, zodat de beleggingsonderneming een andere leverancier kan selecteren of kan besluiten de diensten zelf uit te voeren. • Blanco is een solide bedrijf met betrokken raad van commissarissen en investeerders, waarmee	

							strategische en financiële stabiliteit goed worden gemonitord en gewaarborgd • De beleggingsonderneming kan een lijst bijhouden van potentiële partijen die (delen van) de dienstverlening van Blanco kunnen overnemen indien noodzakelijk.	
4	Dienstverlener staakt activiteiten	Het risico dat gegevens, systemen en diensten (direct) niet langer beschikbaar zijn zodra een dienstverlener zijn activiteiten staakt. Mogelijk worden de dagelijkse werkzaamheden van de instelling verstoord en is het moeilijk of onmogelijk om gegevens op te vragen.					Input Blanco: • In de overeenkomst is een bepaling opgenomen met betrekking tot exit assistentie • In de overeengekomen is opgenomen dat de data eigendom blijft van beleggingsonderneming en dat bij een beëindigen van de overeenkomt de data naar keuze van de beleggingsonderneming wordt verwijderd of overgedragen. • In geval van een faillissement van Blanco is er contractueel een continuïteitsmaatregel overeengekomen, waarbij een Stichting tijdelijk de dienstverlening van Blanco overneemt, zodat beleggingsonderneming een andere leverancier kan selecteren.	

5	Naleving wet en regelgeving.	De instelling behoudt de verantwoordelijkheid over de uitbestede activiteiten en dient er zorg voor te dragen dat de dienstverlener (en onderaannemers) voldoet aan toepasselijke wet- en regelgeving.					Input Blanco: • In de overeenkomst is opgenomen dat de software van Blanco ontwikkelingen in wet- en regelgeving meeneemt. • De overeenkomst biedt de mogelijkheid om te toetsen of de software voldoet aan wet- en regelgeving en aan de service levels zoals overeengekomen tussen partijen.	
6	Onvoldoende performance / resultaten	De dienstverlener houdt zich niet aan de kwaliteitsnormen of voldoet niet aan de gemaakte afspraken, ook al worden kwantitatieve servicelevels wel gehaald. Of de dienstverlening voldoet aan kwantitatieve service levels, maar de kwaliteitsnormen worden niet gehaald. Of kwalitatieve en kwantitatieve normen worden niet gehaald. Hierbij gaat het om monitoring en evaluatie; certificering, service level rapporten, assurancerapporten, audits.					Input Blanco • Waar mogelijk rapporteert Blanco over service levels en informeert Blanco over ontwikkelingen binnen de organisatie en met betrekking tot het product. • Contractueel is de beleggingsonderneming een ISAE3402 Type II rapport kan opvragen.	

7	Gegevenslocatie	De gegevens vallen onder de wetgeving van de locatie waar ze worden opgeslagen of langs worden geleid. Mogelijk verschilt dergelijke lokale wetgeving van de Nederlandse, wat een risico kan vormen met betrekking tot de eisen inzake vertrouwelijkheid.					Input Blanco: • Met betrekking tot de PMS Module (AIRS) wordt momenteel gebruik gemaakt van een datacenter in Nederland, welke op korte termijn zal worden overgezet naar AWS datacenter. • Met betrekking tot andere producten van Blanco, wordt gebruik gemaakt van AWS en heeft voor het opslaan van gegevens gekozen voor de Frankfurt regio. AWS verplaatst de data van Blanco niet uit de geselecteerde regio's zonder Blanco hiervan op de hoogte te stellen, tenzij dit is vereist om te voldoen aan de wet of verzoeken van overheidsinstanties. AWS voldoet volledig aan de toepasselijke EU-wetgeving inzake gegevensbescherming. • Een verwerkers-overeenkomst is onderdeel van de overeenkomst met Blanco. Deze overeenkomst voldoet aan de eisen van de wet. (AVG)	

8	Scheiding van omgevingen	Voorzieningen kunnen wegvallen die zorgen voor de scheiding van opslag, geheugen, routing en zelfs impact kunnen hebben op de reputatie van de diverse huurders van de gedeelde infrastructuur.					Input Blanco: • Blanco maakt gebruik van AWS en heeft een cloud uitbestedings analyse gemaakt ten aanzien van AWS. De volgende analyse is in dit kader van belang: *Different instances running on the same physical machine are isolated from each other via the Xen hypervisor. AWS is active in the Xen community, which provides awareness of the latest developments. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.* *Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer, so that one customer's data is never unintentionally exposed to another. In addition, memory allocated to guests is scrubbed (set to zero) by the hypervisor when it is*	

							unallocated to a guest. The memory is not returned to the pool of free memory available for new allocations until the memory scrubbing is complete. *In the Blanco-solution there is a logical seperation of data on tenants as well. They cannot cross-interfere because there is no capacity management needed per tenant or per solution.*	
9	Gegevenstoegang	Wordt er op een wettelijk juiste manier met de gegevens omgegaan. Hierbij gaat het om de naleving van de regelgeving, zoals over encryptiestandaarden, beheer van encryptiesleutels, het vierogenbeginsel en authenticatie.					Input Blanco: • Blanco beschikt over een ISAE3402 Type 2 rapport, waar de encryptiestrategie en een acces & identity policy onderdeel van uitmaken.	
10	Cyberaanvallen	Alle risico's die verband houden met cyberaanvallen, zoals DDoS-aanvallen, het onderscheppen of uitlekken van gegevens, social engineering, ongeoorloofde toegang, het ongeoorloofd verkrijgen van rechten en ransomware					Input Blanco: • Blanco maakt gebruik van AWS en heeft een cloud uitbestedings analyse gemaakt ten aanzien van AWS. De volgende analyse is in dit kader van belang: *AWS API endpoints are hosted on large, Internet-scale, world- class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS' networks are multi-homed across a number of providers to achieve Internet access diversity.*	

							Blanco added AWS WAF (Web Application Firewall) for parts of the solution. This will help against DDOS. Also, Blanco can block specific countries if needed.	

Extra risico suggestie Blanco:

11	Back-up verloren	Vanwege onvoldoende fysieke beveiligingsprocedures, kwetsbaarheden, kwetsbaarheden voor gebruikersvoorziening, gebruiker deprovisioning kwetsbaarheden.					Input Blanco: • Blanco maakt gebruik van AWS en heeft een cloud uitbestedings analyse gemaakt ten aanzien van AWS. De volgende analyse is in dit kader van belang: *AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS*	

							data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. *AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.*	