EBA/GL/2019/02

25 februari 2019

Richtsnoeren inzake uitbesteding

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1093/2010[1]. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 spannen bevoegde autoriteiten en financiële instellingen zich tot het uiterste in om aan die richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. Bevoegde autoriteiten als bedoeld in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010 voor wie richtsnoeren gelden, dienen hieraan te voldoen door deze op passende wijze in hun praktijken te integreren (bijvoorbeeld door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer richtsnoeren primair tot instellingen en betalingsinstellingen zijn gericht.

Rapportageverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA vóór (dd.mm.jjjj) ervan in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of, indien dit niet het geval is, wat de redenen van de niet-naleving zijn. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet aan de richtsnoeren te hebben voldaan. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar compliance@eba.europa.eu onder vermelding van "EBA/GL/2019/02". Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteiten te melden of zij aan de richtsnoeren voldoen. Elke verandering in de status van de naleving moet eveneens aan EBA worden gemeld.

4. Kennisgevingen worden overeenkomstig artikel 16, lid 3, van de EBA-verordening op de EBA-website bekendgemaakt.

[1] Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

2. Onderwerp, toepassingsgebied en definities

Onderwerp

5. In deze richtsnoeren worden de regelingen voor interne governance, waaronder solide risicobeheer, gespecificeerd die instellingen, betalingsinstellingen en instellingen voor elektronisch geld dienen in te voeren wanneer zij functies uitbesteden, vooral als het gaat om de uitbesteding van kritieke of belangrijke functies.

6. In de richtsnoeren wordt beschreven hoe de in de het vorige punt genoemde regelingen door de bevoegde autoriteiten worden getoetst en gecontroleerd, in de context van artikel 97 van Richtlijn 2013/36/EU[2] (proces van toetsing en evaluatie door de toezichthouder), artikel 9, lid 3, van Richtlijn 2015/2366/EU[3] en artikel 5, lid 5, van Richtlijn 2009/110/EG[4]; de bevoegde autoriteiten doen dat door na te gaan of de entiteiten waaraan deze richtsnoeren zijn gericht, zich voortdurend aan de voorwaarden van hun vergunning houden.

Geadresseerden

7. Deze richtsnoeren zijn gericht aan de bevoegde autoriteiten als gedefinieerd in artikel 4, lid 1, punt 40, van Verordening (EU) nr. 575/2013[5], met inbegrip van de Europese Centrale Bank ten aanzien van kwesties die verband houden met de taken die Verordening (EU) nr. 1024/2013[6] aan de ECB toewijst, instellingen als gedefinieerd in artikel 4, lid 1, punt 3, van Verordening (EU) 575/2013, betalingsinstellingen als gedefinieerd in artikel 4, punt 4, van Richtlijn (EU) 2015/2366 en instellingen voor elektronisch geld in de zin van artikel 2, punt 1, van Richtlijn 2009/110/EU. Aanbieders van rekeninginformatiediensten die uitsluitend de in bijlage I, punt 8, bij Richtlijn (EU) 2015/2366 vermelde dienst verlenen, vallen niet onder deze richtsnoeren, overeenkomstig artikel 33 van die richtlijn.

---

[2] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG.

[3] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG.

[4] Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG.

[5] Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1).

[6] Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen.

8. In deze richtsnoeren vallen, in geval van verwijzing naar “betalingsinstellingen”, daar ook “instellingen voor elektronisch geld” onder en in geval van verwijzing naar “betalingsdiensten” valt daar ook de “uitgifte van elektronisch geld” onder.

Toepassingsgebied

9. Onverminderd Richtlijn 2014/65/EU[7] en Gedelegeerde Verordening (EU) 2017/565 van de Commissie [8] (die voorschriften bevat voor de uitbesteding door instellingen die beleggingsdiensten en -activiteiten verrichten, en relevante richtsnoeren van de Europese Autoriteit voor effecten en markten inzake beleggingsdiensten en -activiteiten), voldoen instellingen als gedefinieerd in artikel 3, lid 1, punt 3, van Richtlijn 2013/36/EU op individuele, gesubconsolideerde en geconsolideerde basis aan deze richtsnoeren. Van de toepassing op individuele basis kan door bevoegde autoriteiten vrijstelling worden 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. Instellingen die onder Richtlijn 2013/36/EU vallen, voldoen op geconsolideerde en gesubconsolideerde basis aan deze richtlijn en deze richtsnoeren, als uiteengezet in artikel 21 en de artikelen 108 tot en met 110 van Richtlijn 2013/36/EU.

10. Onverminderd artikel 8, lid 3, van Richtlijn (EU) 2015/2366 en artikel 5, lid 7, van Richtlijn 2009/110/EG voldoen betalingsinstellingen en instellingen voor elektronisch geld op individuele basis aan deze richtsnoeren.

11. Bevoegde autoriteiten die voor het toezicht op instellingen, betalingsinstellingen en instellingen voor elektronisch geld verantwoordelijk zijn, voldoen aan deze richtsnoeren.

Definities

12. Tenzij anders aangegeven, hebben de termen die worden gebruikt en gedefinieerd in Richtlijn 2013/36/EU, Verordening (EU) nr. 575/2013, Richtlijn 2009/110/EU, Richtlijn (EU) 2015/2366 en de EBA-richtsnoeren inzake interne governance[9], in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden bovendien de volgende definities:

Uitbesteding	een overeenkomst van om het even welke vorm tussen een instelling, een betalingsinstelling of een instelling voor elektronisch geld en een dienstverlener op grond waarvan deze dienstverlener een proces, een dienst of een activiteit verricht die anders door de instelling,

[7] Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).

[8] Gedelegeerde Verordening (EU) 2017/565 van de Commissie van 25 april 2016 houdende aanvulling van Richtlijn 2014/65/EU van het Europees Parlement en de Raad wat betreft de door beleggingsondernemingen in acht te nemen organisatorische eisen en voorwaarden voor de bedrijfsuitoefening en wat betreft de definitie van begrippen voor de toepassing van genoemde richtlijn (PB L 87 van 31.3.2017, blz. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

	betalingsinstelling of instelling voor elektronisch geld zelf zou worden verricht.
Functie	processen, diensten of activiteiten.
Kritieke of belangrijke functie[10]	een functie die als kritiek of belangrijk wordt beschouwd zoals beschreven in hoofdstuk 4 van deze richtsnoeren.
Onderuitbesteding	een situatie waarin de dienstverlener op grond van een uitbestedingsregeling een uitbestede functie verder overdraagt aan een andere dienstverlener.[11]
Dienstverlener	een derde partij die een uitbesteed proces of een uitbestede dienst of activiteit, of onderdelen daarvan, verricht op grond van een uitbestedingsregeling.
Clouddiensten	diensten geleverd met behulp van cloudcomputing, dat wil zeggen een model om via het netwerk overal eenvoudig op verzoek toegang te verlenen tot een gedeelde pool van configureerbare IT-middelen (bijv. netwerken, servers, opslagmedia, applicaties en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald.
Publieke cloud	cloudinfrastructuur voor vrij gebruik door het algemene publiek.
Private cloud	cloudinfrastructuur voor exclusief gebruik door één instelling of betalingsinstelling.
Gemeenschappelijke cloud	cloudinfrastructuur voor exclusief gebruik door een bepaalde gemeenschap van instellingen, met inbegrip van meerdere instellingen van één groep.
Hybride cloud	cloudinfrastructuur bestaande uit twee of meer onderscheiden cloudinfrastructuren.
Leidinggevend orgaan	het (de) overeenkomstig nationaal recht aangewezen orgaan (organen) van een instelling of betalingsinstelling die de bevoegdheid hebben de strategie, doelstellingen en de algemene richting van de instelling of betalingsinstelling vast te stellen, en die toezicht houden op de bestuurlijke besluitvorming en deze controleert, met inbegrip van de personen

[10] De formulering “kritieke of belangrijke functie” houdt verband met de operationele taken die worden beschreven in Richtlijn 2014/65/EU (MiFID II) en Gedelegeerde Verordening (EU) 2017/565 van de Commissie houdende aanvulling van MiFID II en wordt uitsluitend gebruikt voor uitbesteding; zij houdt geen verband met de definitie van “kritieke functies” met het oog op het kader voor herstel en afwikkeling als gedefinieerd in artikel 2, lid 1, punt 35, van Richtlijn 2014/59/EU (BRRD).

[11] Voor de beoordeling gelden de bepalingen van hoofdstuk 3; in andere EBA-documenten wordt in de Engelse tekst voor onderuitbesteding in plaats van “sub-outsourcing” (zoals in dit document) ook wel “chain of outsourcing” of “chain-outsourcing” gebruikt.

	die het beleid van de instelling of betalingsinstelling daadwerkelijk bepalen, en de bestuurders en personen die voor het beheer van de betalingsinstelling verantwoordelijk zijn.

3. Tenuitvoerlegging

Ingangsdatum

13. Met uitzondering van punt 63, onder b), gelden deze richtsnoeren met ingang van 30 september 2019 voor alle uitbestedingsregelingen die op of na deze datum zijn aangegaan, herzien of gewijzigd. Punt 63, onder b), geldt met ingang van 31 december 2021.

14. Instellingen en betalingsinstellingen herzien bestaande uitbestedingsregelingen en wijzigen deze dienovereenkomstig om ervoor te zorgen dat zij aan deze richtsnoeren voldoen.

15. Wanneer de herziening van uitbestedingsregelingen voor kritieke of belangrijke functies niet op 31 december 2021 is afgerond, brengen instellingen en betalingsinstellingen hun bevoegde autoriteit daarvan op de hoogte, en tevens van de maatregelen die zij hebben gepland om de herziening of de mogelijke exitstrategie te voltooien.

Overgangsbepalingen

16. Instellingen en betalingsinstellingen maken de documentatie voor alle bestaande uitbestedingsregelingen, anders dan voor uitbestedingsregelingen voor aanbieders van clouddiensten, in overeenstemming met deze richtsnoeren gereed na de eerste datum waarop elke bestaande uitbestedingsregeling wordt verlengd, maar uiterlijk 31 december 2021.

Intrekking

17. De uitbestedingsrichtsnoeren van het Comité van Europese bankentoezichthouders (CEBT) van 14 december 2006 en de EBA-aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten[12] worden per 30 september 2019 ingetrokken.

[12] Aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten (EBA/REC/2017/03).

4. Richtsnoeren inzake uitbesteding

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.

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.

20. Bij het toepassen van het evenredigheidsbeginsel nemen instellingen, betalingsinstellingen[13] 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.

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.[14] 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.

---

[13] Betalingsinstellingen raadplegen ook de EBA-richtsnoeren uit hoofde van PSD2 betreffende de gegevens die moeten worden verstrekt voor de vergunning van betaalinstellingen en instellingen voor elektronisch geld en voor de registratie van aanbieders van rekeninginformatiediensten, die op de website van de EBA beschikbaar zijn onder de volgende link: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[14] Zie artikel 4, lid 1, punten 47) en 48) van Verordening (EU) nr. 575/2013 voor het bereik van de consolidatie.

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[15] 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.

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

[15] In overeenstemming met artikel 113, lid 7, van de CRR-verordening is een institutioneel protectiestelsel een contractuele of wettelijke aansprakelijkheidsregeling waardoor de instellingen die bij de regeling zijn aangesloten, beschermd worden en waardoor, zo nodig, met name hun liquiditeit en solventie beschermd worden om faillissement te voorkomen.

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 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.

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.

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.

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.

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).

4 Kritieke of belangrijke functies

29. In de volgende situaties beschouwen instellingen en betalingsinstellingen een functie altijd als kritiek of belangrijk:[16]

    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 solliditeit 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[17] van een bevoegde autoriteit nodig is, als bedoeld in paragraaf 12.1.

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 2014/59[18] en vastgesteld door instellingen op grond van de criteria van de artikelen 6 en 7 van Gedelegeerde Verordening (EU) 2016/778 van de Commissie.[19] Functies die nodig zijn om activiteiten van kernbedrijfsonderdelen of kritieke

[16] Zie ook artikel 30 van Gedelegeerde Verordening (EU) nr. 2017/565 van de Commissie van 25 april 2016 houdende aanvulling van Richtlijn 2014/65/EU van het Europees Parlement en de Raad wat betreft de door beleggingsondernemingen in acht te nemen organisatorische eisen en voorwaarden voor de bedrijfsuitoefening en wat betreft de definitie van begrippen voor de toepassing van genoemde richtlijn.

[17] Zie de activiteiten in bijlage I bij Richtlijn 2013/36/EU.

[18] Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen en tot wijziging van Richtlijn 82/891/EEG van de Raad en de Richtlijnen 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU en 2013/36/EU en de Verordeningen (EU) nr. 1093/2010 en (EU) nr. 648/2012, van het Europees Parlement en de Raad (BRRD) (PB L 173 van 12.6.2014, blz. 190).

Gedelegeerde Verordening (EU) 2016/778 van de Commissie van 2 februari 2016 tot aanvulling van Richtlijn 2014/59/EU van het Europees Parlement en de Raad voor wat betreft de omstandigheden en voorwaarden waaronder de betaling van buitengewone achteraf te betalen bijdragen geheel of gedeeltelijk kan worden opgeschort, en inzake de criteria voor de vaststelling van de activiteiten, diensten en bedrijfsactiviteiten ten aanzien van kritieke functies alsook inzake de criteria voor de vaststelling van de bedrijfsonderdelen en daarmee samenhangende diensten ten aanzien van kernbedrijfsonderdelen (PB L 131 van 20.5.2016, blz. 41).

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.

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[20] 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;

    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;

[20] Zie de werkzaamheden in bijlage I bij Richtlijn 2013/36/EU.

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) 2016/679[21].

[21] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening persoonsgegevens).

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[22], met inbegrip van interne controlemechanismen[23], 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.[24]

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.

34. Instellingen en betalingsinstellingen voldoen aan alle voorschriften van Verordening (EU) 2016/679, ook wat betreft hun regelingen met derden en uitbestedingsregelingen.

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.

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;

---

[22] Instellingen dienen titel V van de EBA-richtsnoeren inzake interne governance te raadplegen.

[23] Zie ook artikel 11 van Richtlijn 2015/2366 (PSD2).

[24] Zie ook de EBA-richtsnoeren inzake ICT en risicobeheer op het gebied van veiligheid (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) en de fundamentele onderdelen van de G7 met betrekking tot het beheer van cyberrisico's in de financiële sector (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

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.

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.

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.

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[25], 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.

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:

[25] Zie ook de technische reguleringsnormen op grond van artikel 8, lid 2, van Richtlijn 2013/36/EU aangaande de informatie die aan de bevoegde autoriteiten moet worden verstrekt in de vergunningaanvraag van kredietinstellingen, en de technische uitvoeringsnormen op grond van artikel 8, lid 3, van Richtlijn 2013/36/EU aangaande standaardformulieren, sjablonen en procedures voor de verstrekking van informatie die voor de vergunningverlening aan kredietinstellingen is vereist (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

Voor betalingsinstellingen zie de EBA-richtsnoeren betreffende de gegevens die moeten worden worden verstrekt voor de vergunning van betaalinstellingen en instellingen voor elektronisch geld en voor de registratie van aanbieders van rekeninginformatiediensten uit hoofde van PSD2 (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_NL.pdf/e5ea7f19-987f-42ae-b997-0f6437f8adae).

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.

7 Uitbestedingsbeleid

41. Het leidinggevend orgaan van een instelling of betalingsinstelling[26] 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.

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;

[26] Zie ook de EBA-richtsnoeren inzake beveiligingsmaatregelen voor operationele en beveiligingsrisico's uit hoofde van PSD2, beschikbaar op: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

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;

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.

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.

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[27].

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.

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 synergieën 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.

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 governance[28]. Instellingen en betalingsinstellingen binnen een groep of institutioneel protectiestelsel kunnen wat betreft hun uitbestede functies steunen op centraal opgestelde bedrijfscontinuïteitsplannen.

[27] Betalingsinstellingen kunnen hun beleid ook op deze richtsnoeren afstemmen.

[28] Beschikbaar op: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

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.

10 Interne auditfunctie

50. De activiteiten van de interne auditfunctie[29] omvatten, op grond van een op risico's gebaseerde aanpak, een onafhankelijke toetsing van uitbestede activiteiten. Het auditplan [30] en -programma behelzen in het bijzonder de uitbestedingsregelingen voor kritieke of belangrijke functies.

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.

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.

[29] Wat betreft de verantwoordelijkheden van de interne auditfunctie dienen instellingen hoofdstuk 22 van de EBA-richtsnoeren inzake interne governance te raadplegen (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) en betalingsinstellingen dienen richtsnoer 5 van de EBA-richtsnoeren betreffende de vergunning van betaalinstellingen te raadplegen (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[30] Zie ook de EBA-richtsnoeren inzake de procedure voor toetsing en evaluatie door de toezichthouder: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

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.

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.

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.

56. Instellingen en betalingsinstellingen stellen op verzoek het volledige register van alle bestaande uitbestedingsregelingen[31] 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).

[31] Zie ook de EBA-richtsnoeren inzake het proces van toetsing en evaluatie door de toezichthouder, beschikbaar op: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

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.

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.

59. Instellingen en betalingsinstellingen [32] 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.

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).

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.

[32] Zie ook de EBA-richtsnoeren voor de melding van grote incidenten uit hoofde van PSD2, beschikbaar op: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

12.1 Toezichtsvoorwaarden voor uitbesteding

62. Instellingen en betalingsinstellingen zorgen ervoor dat de uitbesteding van functies van bankactiviteiten[33] 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.

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

[33] Zie artikel 9 van de CRD-richtlijn over het verbod op het bedrijfsmatig aantrekken van deposito's of van andere terugbetaalbare gelden van het publiek voor personen of voor ondernemingen die geen kredietinstelling zijn.

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.

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.

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.

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.

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.

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 potentiële 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.

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.

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.

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.

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.

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.

13 Contractfase

74. De rechten en plichten van de instelling, de betalingsinstelling en de dienstverlener worden duidelijk afgebakend en in een schriftelijke overeenkomst vastgelegd.

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 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.

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.

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.[34]

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.

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.

80. Instellingen en betalingsinstellingen zorgen ervoor dat de dienstverlener op passende wijze toezicht op de onderdienstverleners houdt, conform het beleid dat de instelling of betalingsinstelling heeft vastgesteld. Als de voorgestelde onderuitbesteding materiële nadelige effecten op de uitbestedingsregeling voor een kritieke of belangrijke functie kan hebben of tot een forse toename van het risico zou leiden, onder meer wanneer niet aan de voorwaarden van punt 79 zou worden voldaan, oefent de instelling of betalingsinstelling haar recht uit om

[34] Zie artikel 28 van Verordening (EU) 2016/679.

bezwaar tegen de onderuitbesteding te maken, als een dergelijk recht is overeengekomen, en/of beëindigt zij het contract.

13.2 Beveiliging van gegevens en systemen

81. Instellingen en betalingsinstellingen zorgen ervoor dat dienstverleners, waar relevant, aan de juiste IT-beveiligingsnormen voldoen.

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.

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.

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).

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.

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.

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.

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.

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.

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.[35]

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;

[35] Voor instellingen zie hoofdstuk 22 van de EBA-richtsnoeren inzake interne governance: https://eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_NL.pdf/e75e420e-26a2-4743-99f0-a752f6dbc959

b. door de dienstverlener verstrekte externe certificeringen en externe of interne auditverslagen.

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.

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.

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.[36] Met inachtneming van titel I beschikken betalingsinstellingen eveneens over interne ICT-controlemechanismen, inclusief veiligheidscontrole en risicobeperkende maatregelen in verband met ICT.

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.

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.

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.

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:

    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

[36] Zie ook de EBA-richtsnoeren inzake het ICT-risico: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

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.

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.

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.

101. Instellingen en betalingsinstellingen betrachten de nodige bekwaamheid, zorgvuldigheid en toewijding wanneer zij uitbestedingsregelingen bewaken en beheren.

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.

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.

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.

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.

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 [37]; 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.

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:

[37] Instellingen en betalingsinstellingen hebben passende bedrijfscontinuïteitsplannen voor de uitbesteding van kritieke of belangrijke functies; 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 governance.

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.

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.

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.

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.

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.

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.

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.

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.

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.

116. Tijdens hun beoordeling houden bevoegde autoriteiten rekening met alle risico's, met name:[38]

a. de operationele risico's[39] 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.

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[40] die zij tijdens de beoordeling in kaart hebben gebracht.

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

[38] Voor instellingen die onder Richtlijn 2013/36/EU vallen, zie ook de EBA-richtsnoeren inzake SREP: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Zie ook de EBA-richtsnoeren inzake het ICT-risico: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

[40] Zoals gedefinieerd in artikel 2, lid 1, punt 35, van de BRRD.

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.

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.