EBA/REC/2017/03

28/03/2018

Aanbevelingen

inzake uitbesteding aan aanbieders van clouddiensten

1. Naleving en rapportageverplichtingen

Status van deze aanbevelingen

1. Dit document bevat aanbevelingen 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 de aanbevelingen te voldoen.

2. De aanbevelingen 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 aanbevelingen 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 aanbevelingen primair tot instellingen zijn gericht.

Kennisgevingsverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA uiterlijk op 28.05.2018 ervan in kennis of zij aan deze aanbevelingen 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 aanbevelingen te voldoen. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar compliance@eba.europa.eu onder vermelding van "EBA/REC/2017/03". Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteiten te melden of zij aan de aanbevelingen voldoen. Elke verandering in de status van naleving wordt eveneens aan EBA 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 en toepassingsgebied

1. Deze aanbevelingen vormen een nadere specificatie van de voorwaarden voor uitbesteding zoals bedoeld in de richtsnoeren van het CEBT voor uitbesteding van 14 december 2006 en zijn van toepassing op uitbesteding door instellingen zoals gedefinieerd in artikel 4, lid 1, punt 3, van Verordening (EU) nr. 575/2013 aan aanbieders van clouddiensten.

Adressaten

2. Deze aanbevelingen zijn gericht aan bevoegde autoriteiten als gedefinieerd in artikel 4, lid 2, onder i), van Verordening (EU) nr. 1093/2010 en aan instellingen als gedefinieerd in artikel 4, lid 1, punt 3, van Verordening (EU) nr. 575/2013.[2]

Definities

3. Tenzij anders aangegeven, hebben de termen die in Richtlijn 2013/36/EU[3] over kapitaalvereisten en in de richtsnoeren van het CEBT worden gebruikt en gedefinieerd, dezelfde betekenis in deze aanbeveling. In deze aanbevelingen gelden bovendien de volgende definities:

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 (bv. netwerken, servers, opslagmedia, applicaties en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald.
Public cloud	Cloudinfrastructuur voor vrij gebruik door het algemene publiek.
Private cloud	Cloudinfrastructuur voor exclusief gebruik door één instelling.
Community cloud	Cloudinfrastructuur voor exclusief gebruik door een bepaalde gemeenschap van instellingen, met inbegrip van meerdere instellingen binnen één groep.

[2] 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.

[3] 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.

Hybride cloud	Cloudinfrastructuur bestaande uit twee of meer onderscheiden cloudinfrastructuren.

3. Uitvoering

Datum van toepassing

5. Deze aanbevelingen zijn van toepassing met ingang van 1 juli 2018.

4. Aanbevelingen inzake uitbesteding voor aanbieders van clouddiensten

4.1 Beoordeling van de materialiteit

1. Alvorens over te gaan tot het uitbesteden van haar activiteiten, gaat de instelling na welke activiteiten aangemerkt moeten worden als materieel. Instellingen moeten deze materialiteitsbeoordeling uitvoeren op basis van richtsnoer 1(f) van het CEBT, waarbij zij in het specifieke geval van uitbesteding aan aanbieders van clouddiensten al het volgende in acht neemt:

    (a) het kritische karakter en het profiel van inherente risico's van de uit te besteden activiteiten, d.w.z. de vraag of de activiteiten essentieel zijn voor de bedrijfscontinuïteit / de levensvatbaarheid van de instelling en haar verplichtingen jegens haar klanten;

    (b) het directe operationele effect van onderbrekingen en de daarmee gepaard gaande juridische risico's en reputatierisico's;

    (c) het effect dat een verstoring van de activiteit kan hebben op de verwachte inkomsten van de instelling;

    (d) het effect dat een schending van de vertrouwelijkheid of verlies van de integriteit van gegevens kan hebben op de instelling en haar klanten.

4.2 Verplichting om toezichthouders afdoende te informeren

2. Uitbestedende instellingen dienen de bevoegde autoriteiten afdoende te informeren over materiële activiteiten die zij wensen uit te besteden aan aanbieders van clouddiensten. De instellingen doen dit op basis van paragraaf 4.3 van de CEBT-richtsnoeren en stellen in elk geval de volgende informatie beschikbaar aan de bevoegde autoriteiten:

    (a) de naam van de aanbieder van clouddiensten en (indien van toepassing) de naam van de moedermaatschappij;
    (b) een beschrijving van de uit te besteden activiteiten en gegevens;
    (c) het land of de landen waar de dienst zal worden verleend (met inbegrip van de plaats van de gegevens);
    (d) de aanvangsdatum van de dienstverlening;
    (e) de datum van laatste verlenging van de overeenkomst (indien van toepassing);
    (f) het toepasselijk recht van de overeenkomst;
    (g) de einddatum van de dienstverlening of de eerstvolgende datum van verlenging (indien van toepassing).

3. Naar aanleiding van de conform punt 2 verstrekte informatie kan de bevoegde autoriteit de uitbestedende instelling verzoeken om aanvullende informatie over haar risicoanalyse van de uit te besteden materiële activiteiten vragen, zoals:

    (a) of de aanbieder van clouddiensten een bedrijfscontinuïteitsplan heeft dat geschikt is voor de aan de uitbestedende instelling te verlenen diensten;
    (b) of de uitbestedende instelling een exitstrategie heeft voor het geval van beëindiging door een van de partijen of verstoring van de dienstverlening door de aanbieder;
    (c) of de uitbestedende instelling de vaardigheden en middelen onderhoudt voor passende monitoring van de uitbestede activiteiten.

4. De uitbestedende instelling houdt op instellings- en groepsniveau een register bij met informatie over al haar materiële en niet-materiële activiteiten die zijn uitbesteed aan aanbieders van clouddiensten. Desgevraagd verstrekt de uitbestedende instelling aan de bevoegde autoriteit een kopie van de uitbestedingsovereenkomst en bijbehorende in dat register opgenomen informatie, ongeacht of zij de uitbestede activiteit aan de aanbieder van clouddiensten als materieel heeft beoordeeld of niet.

5. In voornoemd register wordt minimaal de volgende informatie bijgehouden:

    (a) de informatie genoemd onder punt 2(a) tot en met (g), voor zover die niet al is verstrekt;
    (b) het type uitbesteding (model voor de clouddienstverlening en het soort cloud, d.w.z. public/private/hybride/community);
    (c) de partijen aan wie clouddiensten worden verleend uit hoofde van de uitbestedingsovereenkomst;
    (d) bewijs dat de uitbesteding is goedgekeurd door het leidinggevend orgaan of haar gedelegeerde comités, indien van toepassing;
    (e) de namen van onderaannemers, indien van toepassing;
    (f) het land waar de aanbieder van de clouddiensten / de voornaamste onderaannemer is gevestigd;
    (g) of de beoordeling van de uitbesteding materieel is (ja/nee);
    (h) de datum waarop de instelling de laatste materialiteitsanalyse voor de uitbestede activiteiten heeft uitgevoerd;
    (i) of de aanbieder van clouddiensten / onderaannemer (s) tijd kritische bedrijfsactiviteiten ondersteund (ja/nee) clouddiensten;
    (j) beoordeling of er een alternatieve aanbieder is voor de clouddiensten (eenvoudig, moeilijk of onmogelijk);
    (k) gegevens van een alternatieve aanbieder, indien mogelijk;
    (l) de datum van de laatste risicobeoordeling van de uitbestedings- of onderuitbestedingsovereenkomst.

4.3 Toegangs- en auditrecht

Voor instellingen

6. Uitbestedende instellingen zien er overeenkomstig richtsnoer 8(2)(g) van het CEBT op toe dat zij bij het uitbesteden van clouddiensten beschikken over een schriftelijke overeenkomst met de aanbieder van clouddiensten waarin deze zich ertoe verplicht:

   (a) de instelling, een daartoe door de instelling aangewezen derde en de wettelijke auditor van de instelling volledige toegang te verlenen tot zijn bedrijfspanden (hoofdkantoor en operationele centra), met inbegrip van alle voorzieningen, systemen, netwerken en data die hij gebruikt om de uitbestede diensten te leveren (toegangsrecht);

   (b) de instelling, een daartoe door de instelling aangewezen derde en de wettelijke auditor van de instelling onbeperkt auditrecht en controle op de uitbestede diensten te verlenen (auditrecht).

7. De feitelijke uitoefening van het toegangsrecht en het auditrecht mag niet worden belet of beperkt door contractuele regelingen. Indien de omgeving van een andere klant in gevaar zou komen door de uitvoering van een audit of het gebruik van bepaalde auditmethoden, worden alternatieven overeengekomen om de door de instelling vereiste zekerheid te waarborgen.

8. De uitbestedende instelling oefent haar auditrecht en toegangsrecht risico gebaseerd uit. Een uitbestedende instelling die niet beschikt over eigen auditmiddelen, zou ten minste het gebruik van één van de volgende instrumenten moeten overwegen:

   (a) Gemeenschappelijke audits die samen met andere klanten van dezelfde aanbieder van clouddiensten worden georganiseerd en door deze klanten of een door hen aangestelde derde worden uitgevoerd om de auditmiddelen efficiënter te gebruiken en de organisatorische last voor de klanten en de aanbieder van clouddiensten te verminderen;

   (b) Door de aanbieder van clouddiensten verstrekte externe certificeringen of externe of interne auditrapporten, mits:

      i. de uitbestedende instelling erop toeziet dat de certificering of het auditrapport geldig is voor de systemen (d.w.z. processen, applicaties, infrastructuur, datacenters, enz.) en controles die zij als kritisch noodzakelijk heeft aangemerkt bij de aanbieder;
      ii. de uitbestedende instelling de certificering of het auditrapport continu grondig beoordeelt en zich er met name van verzekert dat toekomstige versies van een auditrapport nog geldig zijn voor kritisch noodzakelijke controles, en mits zij verifieert of de certificering of het auditrapport niet verouderd is;
      iii. de uitbestedende instelling tevreden is over de geschiktheid van de certificerende of controlerende partij (bv. met betrekking tot roulering van de certificerende of controlerende organisatie, kwalificaties, deskundigheid, herhaling van de uitvoering / controle van bewijsstukken in het onderliggende auditdossier);

iv. de certificeringen zijn afgegeven en de audits zijn uitgevoerd overeenkomstig algemeen aanvaarde normen en zijn gebaseerd op een toetsing van de operationele doeltreffendheid van de kritisch noodzakelijke controles;

v. de uitbestedende instelling contractueel gerechtigd is te verzoeken om uitbreiding van de reikwijdte van de certificering of het auditrapport tot systemen en/of controles die relevant zijn. Het aantal en de frequentie van dergelijke verzoeken moeten redelijk zijn en vanuit het oogpunt van risicobeheer gerechtvaardigd zijn.

9. Aangezien cloudoplossingen technisch bijzonder complex zijn, verifieert de uitbestedende instelling dat het personeel dat de audit verricht – haar eigen interne auditors of de namens haar handelende pool van auditors dan wel de door de aanbieder van clouddiensten aangestelde auditors – c.q. het personeel dat de externe certificering of het externe auditrapport van de aanbieder evalueert, beschikt over de juiste kennis en vaardigheden om audits en/of beoordelingen van cloudoplossingen op een doeltreffende, toepasselijke wijze te verrichten.

Voor bevoegde autoriteiten

10. Uitbestedende instellingen dienen er overeenkomstig richtsnoer 8(2)(h) van het CEBT op toe te zien dat zij bij het uitbesteden van clouddiensten beschikken over een schriftelijke overeenkomst met de aanbieder van clouddiensten waarin deze zich ertoe verplicht:

(a) de bevoegde autoriteit die toezicht houdt op de uitbestedende instelling (of een door die autoriteit daartoe aangestelde derde), volledige toegang te verlenen tot de bedrijfspanden van de aanbieder (hoofdkantoor en operationele centra), met inbegrip van alle voorzieningen, systemen, netwerken en gegevens die hij gebruikt om de uitbestede diensten te leveren (toegangsrecht);

(b) de bevoegde autoriteit die toezicht houdt op de uitbestedende instelling (of een door die autoriteit daartoe aangestelde derde), onbeperkte rechten voor onderzoek en controle van de uitbestede diensten te verlenen (onderzoeksrecht).

11. De uitbestedende instelling zorgt ervoor dat de contractuele regelingen haar bevoegde autoriteit niet belemmeren bij het uitvoeren van haar functie en het verwezenlijken van haar doelstellingen als toezichthouder.

12. Informatie die bevoegde autoriteiten verkrijgen in het kader van de uitoefening van het toegangs- en onderzoeksrecht is onderworpen aan de voorschriften met betrekking tot beroepsgeheim en vertrouwelijkheid van artikel 53 en volgende van Richtlijn 2013/36/EU (CRD IV). Het is belangrijk dat bevoegde autoriteiten geen contractuele regelingen of andere verplichtingen aangaan die hen beletten zich te houden aan de EU-wetgeving inzake vertrouwelijkheid, beroepsgeheim en de uitwisseling van informatie.

13. Op grond van de bevindingen van haar onderzoek gaat de bevoegde autoriteit over tot het adresseren van eventuele vastgestelde tekortkomingen, zo nodig door rechtstreeks maatregelen op te leggen aan de uitbestedende instelling.

4.4 In het bijzonder voor het toegangsrecht

14. De in paragrafen 6 en 10 bedoelde overeenkomst bevat de volgende bepalingen:

(a) De partij die gebruik wil maken van haar toegangsrecht (instelling, bevoegde autoriteit, controleur of namens de instelling of de bevoegde autoriteit handelende derde) neemt een redelijke termijn in acht om kennis te geven van haar voornemen een bepaald bedrijfspand te bezoeken, tenzij tijdige kennisgeving vanwege een nood- of crisissituatie niet mogelijk is;

(b) De aanbieder van clouddiensten moet zijn volledige medewerking te verlenen aan de desbetreffende bevoegde autoriteiten en aan de instelling en haar controleur in verband met het bezoek ter plaatse.

4.5 Beveiliging van gegevens en systemen

15. Zoals staat te lezen in richtsnoer 8(2)(e) van het CEBT, dient de uitbestedingsovereenkomst de verlener van de uitbestede diensten ertoe te verplichten de vertrouwelijkheid van de door de financiële instelling doorgegeven informatie te beschermen. Overeenkomstig richtsnoer 6(6)(e) van het CEBT wordt van instellingen verwacht dat zij maatregelen treffen om de continuïteit van door verleners van uitbestede diensten geleverde diensten te waarborgen. Richtsnoeren 8(2)(b) en 9 van het CEBT verwachten van de uitbestedende instellingen hun kwaliteits- en prestatievereisten vast te leggen in schriftelijke uitbestedingsovereenkomsten en dienstverleningsovereenkomsten. Deze beveiligingsaspecten moeten continu gemonitord worden (richtsnoer 7).

16. Alvorens over te gaan tot uitbesteding en om haar beslissing te onderbouwen, doet de instelling hiertoe ten minste het volgende:

(a) zij inventariseert en classificeert haar activiteiten, processen en bijbehorende gegevens en systemen en deelt deze in naar gevoeligheid en benodigde bescherming;

(b) zij selecteert, op basis van een grondige risicobeoordeling, de activiteiten, processen en bijbehorende gegevens en systemen die in beginsel in aanmerking komen voor uitbesteding aan een aanbieder van clouddiensten;

(c) zij definieert, en neemt besluiten over, passende bescherming voor 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 clouduitbesteding. Verder gaat de instelling 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 het management van het sleutelbeheer.

17. Vervolgens zorgt de instelling voor een schriftelijke overeenkomst met de aanbieder van clouddiensten waarin onder andere de verplichtingen van laatstgenoemde uit hoofde van 16(c) hierboven zijn opgenomen.

18. De instelling monitort de uitvoering van de activiteiten en de getroffen beveiligingsmaatregelen, met inbegrip van incidenten, continu overeenkomstig richtsnoer 7 van het CEBT, toetst de uitbesteding van activiteiten aan het bepaalde in bovenstaande paragrafen en treft waar nodig onmiddellijk corrigerende maatregelen.

4.6 Plaats van de gegevens en gegevensverwerking

19. Zoals vermeld in richtsnoer 4(4) van het CEBT, dient de instelling extra voorzichtig te zijn bij het aangaan en beheren van uitbestedingsovereenkomsten buiten de EER vanwege mogelijke risico's ten aanzien van de gegevensbescherming en de doeltreffendheid van het toezicht door de toezichthouder.

20. De uitbestedende instelling gaat in haar afwegingen ten aanzien van uitbesteding naar een cloudomgeving uit van de risico's die kunnen samengaan met de plaats van de gegevens en de gegevensverwerking. De beoordeling adresseert de mogelijke gevolgen van risico's, met inbegrip van juridische risico's en nalevingskwesties, en beperkingen van het toezicht in verband met de landen waar de uitbestede diensten (waarschijnlijk) worden geleverd en waar de gegevens (waarschijnlijk) worden opgeslagen. De beoordeling gaat in bredere zin in op de stabiliteit van de politiek en veiligheid in de betrokken rechtsgebieden, de aldaar vigerende wetgeving (met inbegrip van die voor gegevensbescherming) en de voorzieningen voor handhaving aldaar, met inbegrip van het insolventierecht dat van toepassing zou zijn bij niet-naleving door een aanbieder van clouddiensten. De uitbestedende instelling waarborgt dat die risico's binnen aanvaardbare grenzen blijven, overeenkomstig de materialiteit van de uitbestede activiteit.

4.7 Onderuitbesteding

21. In richtsnoer 10 van het CEBT worden instellingen gewezen op de risico's die gepaard gaan met onderuitbesteding; daarvan is sprake wanneer de verlener van de uitbestede diensten elementen van die diensten op zijn beurt aan derde dienstverleners uitbesteedt. Voor de uitbestedende instelling is onderuitbesteding alleen aanvaardbaar als de onderaannemer eveneens volledig voldoet aan de bestaande verplichtingen tussen de uitbestedende instelling en de verlener van de uitbestede diensten. Bij onderuitbesteding treft de uitbestedende instelling passende maatregelen om zich in te dekken tegen het risico dat de verlener van de uitbestede diensten niet goed in staat zou zijn om zijn verplichtingen uit hoofde van de uitbestedingsovereenkomst na te komen indien de onderaannemer de in onderuitbesteding gegeven diensten niet of niet adequaat verleent.

22. De uitbestedingsovereenkomst tussen de uitbestedende instelling en de aanbieder van clouddiensten vermeldt alle soorten activiteiten die zijn uitgesloten van onderuitbesteding en bepaalt dat laatstgenoemde volledig verantwoordelijk blijft voor (het toezicht op) de in onderuitbesteding gegeven diensten.

23. Voorts verplicht de uitbestedingsovereenkomst de aanbieder van clouddiensten de uitbestedende instelling in kennis te stellen van alle voorgenomen belangrijke wijzigingen van de in de oorspronkelijke overeenkomst genoemde onderaannemer(s) of in onderuitbesteding gegeven diensten die ertoe zouden kunnen leiden dat de aanbieder minder goed in staat is zijn verplichtingen uit hoofde van de uitbestedingsovereenkomst na te komen. De kennisgevingstermijn voor dergelijke wijzigingen wordt vooraf contractueel zodanig bepaald dat

de uitbestedende instelling in staat is de risico's als gevolg van de voorgestelde wijzigingen van de onderaannemer(s) of de in onderuitbesteding gegeven diensten te beoordelen voordat zij daadwerkelijk van kracht worden.

24. De uitbestedende instelling kan de overeenkomst beëindigen als zij de risico's als gevolg van de voorgenomen wijzigingen van de onderaannemer(s) of de in onderuitbesteding gegeven diensten als ongunstig beoordeelt.

25. De uitbestedende instelling evalueert en monitort de uitvoering van de algehele dienstverlening continu, ongeacht of de diensten worden verleend door de aanbieder van clouddiensten of door diens onderaannemer(s).

4.8 Continuïteitsplannen en exitstrategieën

26. Zoals is vermeld in richtsnoeren 6.1, 6(6)(e) en 8(2)(d) van het CEBT, moet de uitbestedende instelling regelingen plannen en implementeren om de continuïteit van haar activiteiten te waarborgen voor het geval dat de verlener van de uitbestede diensten geen diensten of diensten van een onaanvaardbaar niveau verleend. Die regelingen omvatten een continuïteitsplan en een duidelijk omschreven exitstrategie. Daarnaast bevat de uitbestedingsovereenkomst een bepaling voor beëindiging en exitbeheer die het mogelijk maakt de activiteiten die de verlener van de uitbestede diensten verricht over te dragen aan een andere aanbieder van uitbestede diensten of weer bij de uitbestedende instelling onder te brengen.

27. De uitbestedende instelling zorgt er verder voor dat zij regelingen voor uitbesteding van clouddiensten zo nodig kan beëindigen zonder dat dit de dienstverlening al te veel verstoort of nadelige gevolgen heeft voor haar naleving van de regelgeving, en zonder dat dit de continuïteit en kwaliteit van haar dienstverlening aan klanten in het gedrang brengt. Daartoe doet de uitbestedende instelling het volgende:

    (a) zij ontwikkelt en implementeert exitplannen die volledig, gedocumenteerd en waar nodig voldoende getoetst zijn;

    (b) zij zoekt alternatieve oplossingen en stelt overgangsplannen op waarmee zij bestaande activiteiten en gegevens beheerst en op voldoende geteste wijze bij de aanbieder van clouddiensten kan weghalen en naar die oplossingen kan overbrengen, met oog voor mogelijke problemen met de plaats van gegevens en instandhouding van de bedrijfscontinuïteit tijdens de overgangsfase;

    (c) zij waarborgt dat de uitbestedingsovereenkomst de aanbieder van clouddiensten ertoe verplicht de uitbestedende instelling in geval van beëindiging van de uitbestedingsovereenkomst voldoende te ondersteunen om de activiteit op ordelijke wijze over te brengen naar een andere aanbieder of weer onder direct beheer van de uitbestedende instelling te brengen.

28. Bij het bepalen van een exitstrategie neemt de uitbestedende instelling het volgende in overweging:

    (a) zij ontwikkelt belangrijke risico-indicatoren om te identificeren wanneer de dienstverlening onaanvaardbaar is;

    (b) zij voert een businessimpactanalyse uit van de potentiële bedrijfsschade in verhouding tot de uitbestede activiteiten om na te gaan welke personele en materiële middelen nodig zouden zijn om het exitplan uit te voeren en hoe lang dat zou duren;

    (c) zij wijst taken en verantwoordelijkheden toe voor het beheer van exitplannen en overgangsactiviteiten;

    (d) zij stelt criteria op om te bepalen of de overgang geslaagd is.

29. De uitbestedende instelling past indicatoren voor de eventuele inwerkingstelling van het exitplan toe in het kader van haar continue monitoring van, en toezicht op de door de aanbieder van clouddiensten verleende diensten.