EBA/REC/2017/03

28/03/2018

Suosituksia

ulkoistamisesta pilvipalveluihin

1. Noudattamista ja ilmoittamista koskevat velvoitteet

Näiden suositusten asema

1. Tämä asiakirja sisältää suosituksia, jotka on annettu asetuksen (EU) N:o 1093/2010[1] 16 artiklan nojalla. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan mukaan toimivaltaisten viranomaisten ja finanssilaitosten on kaikin tavoin pyrittävä noudattamaan suosituksia.

2. Suosituksissa esitetään Euroopan pankkiviranomaisen näkemys Euroopan finanssivalvojien järjestelmässä noudatettavista asianmukaisista valvontakäytännöistä tai siitä, miten unionin lainsäädäntöä on sovellettava tietyllä alalla. Asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdassa määriteltyjen toimivaltaisten viranomaisten, joihin suosituksia sovelletaan, tulisi noudattaa suosituksia sisällyttämällä ne tarpeen mukaan valvontakäytäntöihinsä (esim. muuttamalla lainsäädäntöään tai valvontamenettelyjään). Tämä koskee myös suosituksia, jotka on suunnattu ensisijaisesti laitoksille.

Raportointivaatimukset

3. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan nojalla toimivaltaisten viranomaisten on ilmoitettava Euroopan pankkiviranomaiselle viimeistään 28/05/2018, noudattavatko ne tai aikovatko ne noudattaa näitä suosituksia, sekä syyt niiden noudattamatta jättämiseen. Jos ilmoitusta ei toimiteta tähän määräaikaan mennessä, Euroopan pankkiviranomainen katsoo, etteivät toimivaltaiset viranomaiset noudata ohjeita. Ilmoitukset toimitetaan lomakkeella, joka on saatavissa Euroopan pankkiviranomaisen sivustolta, lähettämällä se osoitteeseen compliance@eba.europa.eu. Viitteeksi merkitään ”EBA/REC/2017/03”. Ilmoituksen voi lähettää ainoastaan henkilö, jolla on asianmukaiset valtuudet ilmoittaa ohjeiden tai suositusten noudattamisesta toimivaltaisen viranomaisen puolesta. Myös niiden noudattamisen osalta tehtävistä muutoksista on ilmoitettava Euroopan pankkiviranomaiselle.

4. Ilmoitukset julkaistaan Euroopan pankkiviranomaisen verkkosivustolla 16 artiklan 3 kohdan mukaisesti.

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1093/2010, annettu 24 päivänä marraskuuta 2010 Euroopan valvontaviranomaisen (Euroopan pankkiviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/78/EY kumoamisesta (EUVL L 331, 15.12.2010, s.12).

2. Sisältö, soveltamisala ja määritelmät

Aihe ja soveltamisala

1. Näissä suosituksissa täsmennetään Euroopan pankkivalvojien komitean 14. joulukuuta 2006 ulkoistamisesta antamissa ohjeissa (CEBS Guidelines on outsourcing) tarkoitettuja ulkoistamisen ehtoja, ja niitä sovelletaan asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdan 3 alakohdassa tarkoitettuihin laitoksiin niiden ulkoistaessa toimiaan pilvipalvelujen tarjoajille.

Keitä ohjeet koskevat

2. Nämä suositukset on tarkoitettu asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdan i alakohdassa tarkoitetuille toimivaltaisille viranomaisille sekä asetuksen (EU) N:o 575/2013[2] 4 artiklan 1 kohdan 3 alakohdassa tarkoitetuille laitoksille.

Määritelmät

3. Ellei toisin ilmoiteta, näiden suositusten termeillä tarkoitetaan samaa kuin direktiivissä 2013/36/EU[3] ja Euroopan pankkivalvojien komitean ohjeissa käytetyillä ja määritellyillä termeillä. Lisäksi näissä suosituksissa käytetään seuraavia määritelmiä:

Pilvipalvelut	Palveluja, joita tarjotaan pilvipalveluna: Tämä tarkoittaa toimintamallia, joka mahdollistaa yleisesti saatavilla olevan, kätevän, tarpeiden mukaisen pääsyn vapaasti konfiguroitaviin tietotekniikkaresursseihin (esimerkiksi verkkoihin, palvelimiin, tallennustilaan, sovelluksiin ja palveluihin), joita voidaan hankkia ja ottaa käyttöön nopeasti vähäisellä hallinnointityöllä tai vuorovaikutuksella palveluntarjoajan kanssa.
Julkiset pilvipalvelut	Avoimesti käytettävissä oleva julkinen pilvipalveluinfrastruktuuri.
Yksityiset pilvipalvelut	Yksinomaisesti yhden yhtiön käytettävissä oleva pilvipalveluinfrastruktuuri.
Yhteisöpilvipalvelut	Pilvipalveluinfrastruktuuri, joka on yksinomaisesti tietyn yhteisön, kuten yhden konsernin useiden yhtiöiden, käytettävissä.
Hybridipilvipalvelut	Kahdesta tai useammasta erillisestä pilvipalveluinfrastruktuurista koostuva pilvipalveluinfrastruktuuri.

[2] Euroopan parlamentin ja neuvoston asetus (EU) N:o 575/2013, annettu 26 päivänä kesäkuuta 2013, luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvaatimuksista ja asetuksen (EU) N:o 648/2012 muuttamisesta.

[3] Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU, annettu 26 päivänä kesäkuuta 2013, oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta.

3. Täytäntöönpano

Voimaantulopäivä

5. Näitä suosituksia sovelletaan 1. heinäkuuta 2018 alkaen.

4. Suosituksia ulkoistamisesta pilvipalveluihin

4.1 Merkittävyyden arviointi

1. Ulkoistavien yhtiöiden tulisi ennen toimintojensa ulkoistamista arvioida, mitkä toiminnot on katsottava merkittäviksi. Yhtiöiden tulisi tehdä tämä toimintojen merkittävyyden arviointi Euroopan pankkivalvojien komitean ohjeiden (ohjeen 1 kohdan f) mukaisesti. Kun toimintoja ulkoistetaan pilvipalvelujen tarjoajille tulisi erityisesti ottaa huomioon seuraavat asiat:

    (a) ulkoistettavien toimintojen kriittisyys ja niille ominainen riskiprofiili eli se, ovatko ne toimintoja, jotka ovat kriittisiä yhtiön liiketoiminnan jatkuvuuden/kannattavuuden kannalta ja niiden velvoitteiden kannalta, joita yhtiöllä on asiakkaitaan kohtaan

    (b) käyttökeskeytysten suora vaikutus toimintaan ja niihin liittyvät oikeudelliset riskit ja maineriskit

    (c) vaikutus, joka millä tahansa toiminnan häiriöllä voi olla yhtiön tulosnäkymiin

    (d) luottamuksellisuuden rikkoutumista tai tiedon eheyttä koskevan häiriön mahdollinen vaikutusyhtiöön ja sen asiakkaisiin.

4.2 Ilmoitusvelvollisuus valvojille

2. Ulkoistavan yhtiön tulisi ilmoittaa toimivaltaisille viranomaisille merkittävistä toiminnoista, joita se aikoo ulkoistaa pilvipalvelujen tarjoajille. Yhtiöiden tulisi tehdä tämä Euroopan pankkivalvojien komitean ohjeiden (ohjeen 4 kohdan 4.3) perusteella ja antaa toimivaltaisten viranomaisten saataville vähintään seuraavat tiedot:

    (a) pilvipalvelujen tarjoajan nimi ja sen (mahdollisen) emoyhtiön nimi
    (b) kuvaus ulkoistettavista toiminnoista ja tiedoista
    (c) maa, jossa tai maat, joissa palvelu toteutetaan (myös tietojen sijainti)
    (d) palvelun alkamispäivä
    (e) viimeinen sopimuksen uusimispäivä (jos soveltuu)
    (f) sopimukseen sovellettava laki
    (g) palvelun päättymispäivä tai sopimuksen seuraava uusimispäivä (jos soveltuu).

3. Edellisen kohdan mukaisesti toimitettujen tietojen lisäksi toimivaltainen viranomainen voi pyytää ulkoistavalta yhtiöltä lisätietoja sen ulkoistettavia merkittäviä toimintoja koskevasta riskianalyysista, kuten:

    (a) Onko pilvipalvelujen tarjoajalla liiketoiminnan jatkuvuussuunnitelma, joka soveltuu ulkoistavalle yhtiölle tarjottaviin palveluihin?

(b) Onko ulkoistavalla yhtiöllä exit-strategia, mikäli jompikumpi osapuoli päättää sopimuksen tai pilvipalveluntarjoajan palvelujen tarjoaminen keskeytyy?
(c) Onko ulkoistavalla yhtiöllä osaaminen ja resurssit, joita tarvitaan ulkoistettavien toimintojen asianmukaiseen valvontaan?

4. Ulkoistavan yhtiön tulisi pitää ajantasaista rekisteriä kaikista pilvipalvelujen tarjoajalle ulkoistetuista merkittävistä ja muista kuin merkittävistä toiminnoistaan yhtiö- ja konsernitasolla. Ulkoistavan yhtiön tulisi toimittaa toimivaltaisen viranomaisen pyynnöstä sen saataville kopio ulkoistamissopimuksesta ja rekisteriin tallennetut tiedot riippumatta siitä, onko yhtiö arvioinut pilvipalvelujen tarjoajalle ulkoistetun toiminnan merkittäväksi vai ei.

5. Edellisessä kohdassa tarkoitetun rekisterin tulisi sisältää vähintään seuraavat tiedot:

(a) kohdan 2 a–g alakohdissa mainitut tiedot, mikäli niitä ei ole vielä toimitettu
(b) ulkoistamisen tyyppi (pilvipalvelun malli ja pilvipalvelun käytön malli eli onko pilvipalvelu julkinen/yksityinen/hybridi/yhteisö)
(c) ulkoistamissopimuksen nojalla pilvipalveluja vastaanottavat osapuolet
(d) soveltuvin osin todisteet siitä, että hallintoelin tai sen osoittama komitea on hyväksynyt ulkoistamisen
(e) alihankkijoiden nimet, mikäli tällaisia on
(f) maa, johon pilvipalvelujen tarjoaja / pääalihankkija on rekisteröity
(g) tieto siitä, onko ulkoistaminen arvioitu merkittäväksi (kyllä/ei)
(h) päivämäärä, jolloin yhtiö on viimeksi arvioinut ulkoistettujen toimintojen merkittävyyttä
(i) tieto siitä, tukeeko pilvipalvelujen tarjoaja / alihankkija(t) aikakriittisiä liiketoimia (kyllä/ei)
(j) arvio pilvipalvelujen tarjoajan korvattavuudesta (helppoa, vaikeaa tai mahdotonta)
(k) vaihtoehtoisen palveluntarjoajan tunnistaminen, mikäli mahdollista
(l) päivämäärä, jolloin ulkoistamis- ja/tai alihankintajärjestelyjen riskiarviointi on viimeksi tehty.

4.3 Pääsy- ja tarkastusoikeudet

Yhtiöille

6. Euroopan pankkivalvojien komitean ohjeiden (ohjeen 8 kohdan 2 g) perusteella yhtiöiden tulisi käyttäessään pilvipalveluja myös varmistaa, että pilvipalvelujen tarjoajan kanssa on tehty kirjallinen sopimus, jossa pilvipalvelujen tarjoaja sitoutuu velvoitteeseen

(a) tarjota yhtiölle, yhtiön tätä tarkoitusta varten nimeämälle kolmannelle osapuolelle ja yhtiön lakisääteiselle tilintarkastajalle täysi pääsyoikeus sen liiketiloihin (päätoimipaikkoihin ja toimintakeskuksiin), mukaan lukien kaikki laitteet, järjestelmät, verkot ja tiedot, joita käytetään ulkoistettujen palvelujen tarjoamisessa (pääsyoikeus)

(b) antaa yhtiölle, yhtiön tätä tarkoitusta varten nimeämälle kolmannelle osapuolelle ja yhtiön lakisääteiselle tilintarkastajalle rajoittamattomat tarkastusoikeudet ulkoistettuihin palveluihin (tarkastusoikeus).

7. Näiden pääsy- ja tarkastusoikeuksien tehokasta käyttöä ei saisi estää tai rajoittaa sopimusjärjestelyillä. Jos tarkastusten tekeminen tai tiettyjen tarkastusmenetelmien käyttäminen voi aiheuttaa riskin toisen asiakkaan ympäristölle, tulisi sopia vaihtoehtoisista tavoista saavuttaa vastaava yhtiön edellyttämä varmuustaso.

8. Ulkoistavan yhtiön tulisi käyttää tarkastus- ja pääsyoikeuksiaan riskiperusteisesti. Jos ulkoistava yhtiö ei käytä omia tarkastusresurssejaan, sen tulisi harkita vähintään yhtä seuraavista toteutustavoista:

   (a) saman pilvipalvelujen tarjoajan muiden asiakkaiden kanssa järjestettävät yhteiset tarkastukset, jotka kyseiset asiakkaat tai niiden nimittämä kolmas osapuoli tekevät; näin tarkastusresursseja käytetään tehokkaammin ja organisatorinen taakka vähenee sekä asiakkailta että pilvipalvelun tarjoajalta

   (b) pilvipalvelujen tarjoaja antaa saataville kolmannen osapuolen sertifioinnit ja kolmannen osapuolen tai sisäisen tarkastuksen tarkastusraportit edellyttäen, että

      i. ulkoistava yhtiö varmistaa, että sertifioinnin tai tarkastusraportin laajuus kattaa järjestelmät (prosessit, sovellukset, infrastruktuurin, konesalit jne.) ja kontrollit, jotka ulkoistava yhtiö on määrittänyt keskeisiksi
      ii. ulkoistava yhtiö arvioi säännöllisesti ja kattavasti sertifiointien tai tarkastusraporttien sisältöä ja varmistaa erityisesti, että myös tarkastusraportin tulevat versiot kattavat keskeiset kontrollit, sekä varmistaa, että sertifiointi tai tarkastusraportti ei ole vanhentunut
      iii. ulkoistava yhtiö on tyytyväinen sertifioivan tai tarkastuksia tekevän osapuolen soveltuvuuteen (esim. sertifiointi- tai tarkastusyrityksen vaihtamisen, pätevyyden, asiantuntemuksen ja tarkastettaviin tietoihin liittyvien todisteiden tutkimisen uudelleensuorittamisen tai niiden varmentamisen osalta)
      iv. sertifioinnit annetaan ja tarkastukset tehdään yleisesti tunnustettujen standardien perusteella, ja niihin sisältyy käytössä olevien keskeisten kontrollien operatiivisen tehokkuuden testaus
      v. ulkoistavalla yhtiöllä on sopimukseen perustuva oikeus pyytää sertifiointien tai tarkastusraportin tavoitteiden laajentamista asiaankuuluviin järjestelmiin ja/tai kontrolleihin. Tällaisten pyyntöjen määrän ja esittämistiheyden tulisi olla kohtuullinen sekä oikeutettu riskienhallinnan näkökulmasta.

9. Koska pilvipalveluratkaisut ovat teknisesti erittäin monimutkaisia, ulkoistavan yhtiön tulisi varmistaa, että tarkastuksen tekevällä henkilöstöllä – riippumatta siitä, onko kyse sisäisistä tarkastajista vai yhtiön puolesta toimivasta tarkastajaryhmästä vai pilvipalvelujen tarjoajan nimittämistä tarkastajista – tai soveltuvin osin kolmannen osapuolen sertifiointia tai palveluntarjoajan tarkastusraportteja tarkastavalla henkilöstöllä on asianmukainen osaaminen

ja tietämys pilvipalvelujen tehokkaiden ja asiaankuuluvien tarkastusten ja/tai arviointien tekemistä varten.

Toimivaltaisille viranomaisille

10. Euroopan pankkivalvojien komitean ohjeiden (ohjeen 8 kohdan 2 h) perusteella yhtiöiden tulisi ulkoistaessaan pilvipalveluihin varmistaa, että pilvipalvelujen tarjoajan kanssa on tehty kirjallinen sopimus, jossa pilvipalvelujen tarjoaja sitoutuu velvoitteeseen

    (a) tarjota ulkoistavan yhtiön toimintaa valvovalle toimivaltaiselle viranomaiselle (tai kyseisen viranomaisen tätä tarkoitusta varten nimeämälle kolmannelle osapuolelle) täysi pääsyoikeus sen liiketiloihin (päätoimipaikkoihin ja toimipisteisiin), mukaan lukien kaikki laitteet, järjestelmät, verkot ja tiedot, joita käytetään ulkoistettujen palvelujen tarjoamisessa (pääsyoikeus)

    (b) antaa ulkoistavaa yhtiötä valvovalle toimivaltaiselle viranomaiselle (tai kyseisen viranomaisen tätä tarkoitusta varten nimeämälle kolmannelle osapuolelle) rajoittamattomat tarkastusoikeudet ulkoistettuihin palveluihin (tarkastusoikeus).

11. Ulkoistavan yhtiön tulisi varmistaa, että sopimusjärjestelyt eivät estä toimivaltaista viranomaista suorittamasta valvontatehtäväänsä ja tavoitteitaan.

12. Toimivaltaisten viranomaisten pääsy- ja tarkastusoikeuden käyttämisen nojalla saamiin tietoihin tulisi soveltaa direktiivin 2013/36/EY (CRD IV) 53 artiklassa ja sitä seuraavissa artikloissa tarkoitettuja salassapito- ja luottamuksellisuusvaatimuksia. Toimivaltaisten viranomaisten tulisi pidättäytyä tekemästä mitään sopimusjärjestelyjä tai ilmoituksia, jotka estäisivät niitä noudattamasta luottamuksellisuutta, salassapitoa ja tietojenvaihtoa koskevia unionin lainsäädännön säännöksiä.

13. Tarkastusten havaintojen perusteella toimivaltaisen viranomaisen tulisi puuttua tarvittaessa kaikkiin havaittuihin puutteisiin määräämällä toimenpiteitä suoraan ulkoistavalle yhtiölle.

4.4 Pääsyoikeutta koskevat ehdot

14. Edellä 6 ja 10 kohdassa tarkoitettuun sopimukseen tulisi sisällyttää seuraavat ehdot:

    (a) Osapuolen, joka aikoo käyttää pääsyoikeuttaan (yhtiö, toimivaltainen viranomainen, tarkastaja tai yhtiön tai toimivaltaisen viranomaisen puolesta toimiva kolmas osapuoli), tulisi kohtuullisessa ajassa ennen asiaankuuluviin liiketiloihin suunniteltua käyntiä ilmoittaa käynnistä, paitsi jos varhainen ennakkoilmoitus ei ole mahdollista hätä- tai kriisitilanteen vuoksi.

    (b) Pilvipalvelujen tarjoajan tulisi tehdä yhteistyötä toimivaltaisten viranomaisten, yhtiön ja sen tarkastajan kanssa paikalla tehtävän (onsite) käynnin yhteydessä.

4.5 Tietojen ja järjestelmien turvallisuus

15. Kuten Euroopan pankkivalvojien komitean ohjeissa (ohje 8 kohdan 2 e) todetaan, ulkoistamissopimuksessa tulisi velvoittaa ulkoistamispalvelun tarjoaja turvaamaan yhtiön toimittamien tietojen luottamuksellisuus. Euroopan pankkivalvojien komitean ohjeiden (ohjeen 6 kohdan 6 e) mukaisesti yhtiöiden tulisi ottaa käyttöön järjestelyjä, joilla varmistetaan ulkoistamispalvelujen tarjoajien tarjoamien palvelujen jatkuvuus. Euroopan pankkivalvojien ohjeiden (ohjeen 8 kohdan 2 b ja ohjeen 9) perusteella ulkoistavien yhtiöiden laatua ja suorituskykyä koskevat tarpeet tulisi kirjata kirjallisiin ulkoistamissopimuksiin ja palvelutasosopimuksiin. Näitä turvallisuusnäkökohtia tulisi myös valvoa jatkuvasti (ohje 7).

16. Edellä olevan kappaleen tarkoitusten mukaisesti ja tiedottaakseen päätöksestä, yhtiön tulisi ennen ulkoistamista ainakin

    (a) määrittää ja luokitella toimintonsa, prosessinsa ja niihin liittyvät tiedot ja järjestelmät arkaluonteisuuden ja vaaditun suojaustason mukaan

    (b) tehdä perusteellinen riskiperusteinen valinta toiminnoista, prosesseista ja niihin liittyvistä tiedoista ja järjestelmistä, jotka aiotaan ulkoistaa pilvipalveluratkaisuun

    (c) määrittää ja päättää tietojen luottamuksellisuuden asianmukainen suojaustaso, ulkoistettavien toimintojen jatkuvuus sekä tietojen ja järjestelmien eheys ja jäljitettävyys suunnitellun pilvipalveluihin ulkoistamisen puitteissa. Yhtiöiden tulisi myös harkita tarvittaessa erityistoimenpiteitä siirrettävälle tiedolle, muistissa olevalle tiedolle ja säilytyksessä olevalle tiedolle, kuten salausmenetelmien käyttö yhdessä asianmukaisen avaintenhallinta-arkkitehtuurin kanssa.

17. Yhtiöiden tulisi siis varmistaa, että niillä on pilvipalvelujen tarjoajan kanssa kirjallinen sopimus, jossa esitetään muun muassa pilvipalvelujen tarjoajan velvoitteet kohdan 16 (c) mukaisesti.

18. Yhtiöiden tulisi valvoa toimien ja turvallisuustoimenpiteiden suorittamista sekä häiriötilanteita, Euroopan pankkivalvojien komitean ohjeiden (ohjeen 7) mukaisesti jatkuvasti ja tarkistaa tarvittaessa, noudatetaanko toimintojen ulkoistamisessa edellisiä kohtia. Niiden tulisi toteuttaa ripeästi mahdolliset tarvittavat korjaavat toimenpiteet.

4.6 Tietojen ja tietojenkäsittelyn sijainti

19. Kuten Euroopan pankkivalvojien komitean ohjeiden (ohjeen 4 kohdassa 4) todetaan, yhtiön tulisi olla erityisen huolellinen tehdessään ja hallinnoidessaan ETA-alueen ulkopuolisia ulkoistamissopimuksia mahdollisten tietosuojariskien vuoksi ja valvontaviranomaisen suorittaman valvonnan tehokkuuteen liittyvien riskien vuoksi.

20. Ulkoistavan yhtiön tulisi omaksua tietojen ja tietojenkäsittelyn sijaintia koskevissa näkökohdissa riskiperusteinen toimintamalli, kun se ulkoistaa toimintoja pilvipalveluympäristöön. Arvioinnissa tulisi käsitellä mahdollisia riskivaikutuksia, muun muassa oikeudellisia riskejä ja vaatimustenmukaisuuskysymyksiä, sekä valvontarajoituksia, jotka liittyvät maihin, joissa ulkoistettuja palveluja tarjotaan tai joissa niitä todennäköisesti tarjotaan ja joissa tietoja säilytetään tai joissa niitä todennäköisesti säilytetään. Arvioinnin tulisi sisältää pohdintaa kyseessä olevien oikeudenkäyttöalueiden laajemmasta poliittisesta ja turvallisuuteen liittyvästä vakaudesta, kyseisillä oikeudenkäyttöalueilla voimassa olevista laeista (mukaan lukien tietosuojalait) ja kyseisillä oikeudenkäyttöalueilla voimassa olevista lainvalvontasäännöksistä, muun muassa maksukyvyttömyyslain säännöksistä, joita sovellettaisiin, jos pilvipalvelujen tarjoaja joutuisi vararikkoon. Ulkoistavan yhtiön tulisi varmistaa, että nämä riskit pidetään hyväksyttävissä rajoissa, jotka vastaavat ulkoistetun toiminnan merkittävyyttä.

4.7 Ulkoistusketju

21. Kuten Euroopan pankkivalvojien komitean ohjeiden ohjeessa 10 todetaan, yhtiöiden tulisi ottaa huomioon riskit, jotka liittyvät ulkoistusketjuun, jossa palveluntarjoaja, jolle palvelut on ulkoistettu, antaa palvelun osia alihankintaan muille palveluntarjoajille. Ulkoistavan yhtiön tulisi hyväksyä ulkoistusketju vain, jos myös alihankkija noudattaa täysimääräisesti ulkoistavan yhtiön ja palveluntarjoajan, jolle palvelut on ulkoistettu, välillä voimassa olevia velvoitteita. Ulkoistavan yhtiön tulisi lisäksi toteuttaa asianmukaiset toimenpiteet sellaisten alihankintana toteutettavien toimien mahdollisten heikkouden tai laiminlyönnin riskien käsittelemiseksi, jotka vaikuttavat merkittävästi sen palveluntarjoajan, jolle palvelut on ulkoistettu, valmiuksiin täyttää ulkoistamissopimuksen mukaiset velvoitteensa.

22. Ulkoistavan yhtiön ja pilvipalvelujen tarjoajan välisessä ulkoistamissopimuksessa tulisi määritellä kaikki ne toiminnot, jotka on rajattu mahdollisen alihankinnan ulkopuolelle, ja ilmoitettava, että pilvipalvelujen tarjoaja on edelleen täysin vastuussa palveluista, jotka se on antanut alihankintaan, sekä niiden valvonnasta.

23. Ulkoistamissopimuksen tulisi myös sisältää pilvipalvelujen tarjoajan velvoite ilmoittaa ulkoistavalle yhtiölle kaikista suunnitelluista merkittävistä muutoksista, jotka koskevat alkuperäisessä sopimuksessa nimettyjä alihankkijoita tai alihankintaan annettuja palveluja ja jotka voivat vaikuttaa palveluntarjoajan valmiuksiin täyttää ulkoistamissopimuksen mukaiset velvoitteensa. Kyseisiä muutoksia koskevasta ilmoitusajasta tulisi sopia etukäteen sopimuksessa, jotta ulkoistava yhtiö voi tehdä riskinarvioinnin ehdotettujen muutosten

vaikutuksista ennen kuin alihankkijoita tai alihankintana toteutettavia palveluja koskeva todellinen muutos tulee voimaan.

24. Mikäli pilvipalvelujen tarjoaja suunnittelee alihankkijoiden tai alihankintana toteutettavien palvelujen osalta muutoksia, jotka vaikuttaisivat haitallisesti sovitun palvelun riskinarviointiin, ulkoistavalla yhtiöllä tulisi olla oikeus päättää sopimus.

25. Ulkoistavan yhtiön tulisi tarkistaa ja valvoa yleisen palvelun suoritustasoa jatkuvasti riippumatta siitä, tarjoaako palvelun pilvipalvelun tarjoaja vai sen alihankkija.

4.8 Jatkuvuussuunnitelma ja exit-strategia

26. Kuten Euroopan pankkivalvojien komitean ohjeissa (ohjeen 6 kohdassa 6.1 ja 6 e sekä ohjeen 8 kohdassa 2 d) todetaan, ulkoistavan yhtiön tulisi suunnitella ja ottaa käyttöön järjestelyt, joilla se ylläpitää liiketoiminnan jatkuvuutta, mikäli palveluntarjoaja, jolle palvelut on ulkoistettu, ei kykene tarjoamaan palvelua tai palvelu heikentyy tasolle, jota ei voida hyväksyä. Näiden järjestelyjen tulisi sisältää jatkuvuussuunnitelma ja selkeästi määritetty exit-strategia. Ulkoistamissopimukseen tulisi lisäksi kuulua sopimuksen päättämisen ja siitä irtautumisen hallintaa koskeva lauseke, jonka nojalla palveluntarjoajan, jolle palvelut on ulkoistettu, tarjoamat palvelut voidaan siirtää toiselle ulkoistettuja palveluja tarjoavalle palveluntarjoajalle tai palauttaa ulkoistavan yhtiön hallintaan.

27. Ulkoistavan yhtiön tulisi myös varmistaa, että se pystyy tarvittaessa irtautumaan pilvipalvelujen ulkoistamisjärjestelyistä ilman palvelujensa tarjoamisen aiheetonta keskeytymistä tai haitallisia vaikutuksia vaatimuksenmukaisuuden noudattamiseen ja ilman, että se vahingoittaa sen asiakkaille suunnattujen palvelujen tarjoamisen jatkuvuutta ja laatua. Tämän aikaansaamiseksi ulkoistavan yhtiön tulisi

    (a) laatia ja ottaa käyttöön exit-suunnitelmat, jotka ovat kattavia, dokumentoituja ja soveltuvin osin riittävästi testattuja

    (b) tunnistaa vaihtoehtoiset ratkaisut ja laatia siirtymäsuunnitelmia, jotta se voisi poistaa ja siirtää olemassa olevia toimintoja ja tietoja pilvipalvelujen tarjoajalta kyseisiin ratkaisuihin hallitusti ja riittävästi testattuna ja ottaen siinä huomioon tietojen sijaintia koskevat kysymykset ja liiketoiminnan jatkuvuuden säilyttämisen siirtymävaiheen aikana

    (c) varmistaa, että ulkoistamissopimus sisältää pilvipalvelujen tarjoajan velvoitteen tarjota riittävästi tukea ulkoistavalle yhtiölle, jotta toiminto voitaisiin siirtää asianmukaisesti toiselle palveluntarjoajalle tai ulkoistavan yhtiön suoraan hallintaan, mikäli ulkoistamissopimus päätetään.

28. Exit-strategioita laatiessaan ulkoistavan yhtiön tulisi huolehtia seuraavista asioista:

(a) laatia sellaiset keskeiset riski-indikaattorit, joilla määritetään ei-hyväksyttävän palvelun taso

(b) laatia liiketoiminnan vaikutusanalyysi, joka on oikeassa suhteessa ulkoistettuihin toimiin ja jossa määritetään, mitä henkilöresursseja ja muita resursseja tarvitaan exit-suunnitelman toteuttamiseen ja miten paljon aikaa se veisi

(c) nimetä tehtävät ja vastuut exit-suunnitelman ja siirtymävaiheen tehtävien hallinnoimiseksi

(d) määrittää siirtymän onnistumisen kriteerit.

29. Ulkoistavan yhtiön tulisi ottaa jatkuvaan palvelujen seurantaan ja pilvipalvelujen tarjoajan tarjoamien palvelujen valvontaan mukaan sellaisia indikaattoreita, jotka voivat käynnistää exit-suunnitelman.