

EBA/GL/2019/02

25. helmikuuta 2019

Ulkoistamista koskevat ohjeet

1. Noudattamista ja ilmoittamista koskevat velvoitteet

Näiden ohjeiden asema

1. Tämä asiakirja sisältää ohjeita, jotka on annettu asetuksen (EU) N:o 1093/2010¹ 16 artiklan nojalla. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan mukaan toimivaltaisten viranomaisten ja finanssilaitosten tulee kaikin tavoin pyrkiä noudattamaan ohjeita.
2. Ohjeissa esitetään Euroopan pankkiviranomaisen (EPV) näkemys asianmukaisista Euroopan finanssivalvojen järjestelmässä toteutettavista valvontakäytännöistä ja siitä, miten unionin oikeutta tulisi soveltaa tietyissä asioissa. Asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdassa tarkoitettujen toimivaltaisten viranomaisten, joihin näitä ohjeita sovelletaan, tulisi noudattaa ohjeita sisällyttämällä ne tarpeen mukaan käytäntöihinsä (esim. muuttamalla oikeudellista kehystään tai valvontamenettelyjään). Tämä koskee myös ohjeita, jotka on suunnattu ensisijaisesti laitoksille ja maksulaitoksille.

Raportointivaatimukset

3. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan mukaisesti toimivaltaisten viranomaisten tulee ilmoittaa Euroopan pankkiviranomaiselle viimeistään ([pp.kk.vvvv]), että ne noudattavat tai aikovat noudattaa näitä ohjeita tai muussa tapauksessa annettava syyt niiden noudattamatta jättämiseen. Jos ilmoitusta ei toimiteta tähän määräaikaan mennessä, Euroopan pankkiviranomainen katsoo, etteivät toimivaltaiset viranomaiset noudata ohjeita. Ilmoitukset lähetetään Euroopan pankkiviranomaisen verkkosivustolla olevaa lomaketta käyttäen sähköpostitse osoitteeseen compliance@eba.europa.eu. Viitteeksi merkitään "EBA/GL/2019/02". Ilmoituksen voi lähettää ainoastaan henkilö, jolla on asianmukaiset valtuudet ilmoittaa ohjeiden noudattamisesta toimivaltaisen viranomaisen puolesta. Myös ohjeiden noudattamisen osalta tehtävistä muutoksista tulee ilmoittaa 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. Kohde, soveltamisala ja määritelmät

Kohde

5. Näissä ohjeissa määritellään sisäistä hallintoa koskevat järjestelyt, mukaan luettuna asianmukainen riskienhallinta, jotka laitosten, maksulaitosten ja sähköisen rahan liikkeeseenlaskijalaitosten on toteutettava ulkoistaessaan toimintoja erityisesti kriittisten tai tärkeiden toimintojen ulkoistamisen osalta.
6. Ohjeissa määritellään, miten toimivaltaisten viranomaisten tulee arvioida ja valvoa edellisessä kohdassa tarkoitettuja järjestelyjä direktiivin 2013/36/EU² 97 artiklan, vakavaraisuuden arviointiprosessin, direktiivin (EU) 2015/2366³ 9 artiklan 3 kohdan ja direktiivin 2009/110/EY⁴ 5 artiklan 5 kohdan puitteissa täyttämällä velvollisuutensa valvoa sitä, että näiden ohjeiden kohteena olevat laitokset noudattavat jatkuvasti toimilupansa ehtoja.

Keitä ohjeet koskevat

7. Ohjeet on tarkoitettu asetuksen (EU) N:o 575/2013⁵ 4 artiklan 1 kohdan 40 alakohdassa määritellyille toimivaltaisille viranomaisille, Euroopan keskuspankille sille asetuksella (EU) N:o 1024/2013⁶ annettuja tehtäviä koskevilta osin sekä asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdan 3 alakohdassa määritellyille laitoksille, direktiivin (EU) 2015/2366 4 artiklan 4 kohdassa määritellyille maksulaitoksille sekä direktiivin 2009/110/EY 2 artiklan 1 kohdassa tarkoitetuille sähköisen rahan liikkeeseenlaskijalaitoksille. Tilitietopalvelujen tarjoajat, jotka tarjoavat ainoastaan direktiivin (EU) 2015/2366 liitteessä I olevassa 8 kohdassa tarkoitettua palvelua, eivät kuulu näiden ohjeiden soveltamisalaan kyseisen direktiivin 33 artiklan mukaisesti.
8. Näissä ohjeissa kaikilla viittauksilla ”maksulaitoksiin” tarkoitetaan myös ”sähköisen rahan liikkeeseenlaskijalaitoksia” ja kaikilla viittauksilla ”maksupalveluihin” tarkoitetaan myös ”sähköisen rahan liikkeellelaskua”.

² 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 Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta.

⁴ Euroopan parlamentin ja neuvoston direktiivi 2009/110/EY, annettu 16 päivänä syyskuuta 2009, sähköisen rahan liikkeeseenlaskijalaitosten liiketoiminnan aloittamisesta, harjoittamisesta ja toiminnan vakauden valvonnasta, direktiivien 2005/60/EY ja 2006/48/EY muuttamisesta sekä direktiivin 2000/46/EY kumoamisesta.

⁵ 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 (EUVL L 176, 27.6.2013, s. 1).

⁶ Neuvoston asetus (EU) N:o 1024/2013, annettu 15 päivänä lokakuuta 2013, luottolaitosten vakavaraisuusvalvontaan liittyvää politiikkaa koskevien erityistehtävien antamisesta Euroopan keskuspankille.

Soveltamisala

9. Rajoittamatta direktiivin 2014/65/EU⁷ ja komission delegoidun asetuksen (EU) 2017/565⁸ (johon sisältyy sijoituspalveluja tarjoavien ja sijoitustoimintaa harjoittavien laitosten toteuttamaa ulkoistamista koskevia vaatimuksia sekä sijoituspalveluja ja -toimintaa koskevia Euroopan arvopaperimarkkinaviranomaisen antamia asianmukaisia ohjeita) soveltamista, direktiivin 2013/36/EU 3 artiklan 1 kohdan 3 alakohdassa määriteltyjen laitosten tulee noudattaa näitä ohjeita yksilöllisellä, konsolidoidulla ja alakonsolidointiryhmän tasolla. Toimivaltaiset viranomaiset voivat vapauttaa laitoksen yksilöllisen tason soveltamisesta direktiivin 2013/36/EU 21 artiklan tai direktiivin 2013/36/EU 109 artiklan 1 kohdan, luettuna yhdessä asetuksen (EU) N:o 575/2013 7 artiklan kanssa, nojalla. Laitosten, joihin sovelletaan direktiiviä 2013/36/EU, tulee noudattaa kyseistä direktiiviä ja näitä ohjeita konsolidoidulla ja alakonsolidointiryhmän tasolla direktiivin 2013/36/EU 21 artiklan ja 108–110 artiklan mukaisesti.
10. Rajoittamatta direktiivin (EU) 2015/2366 8 artiklan 3 kohdan ja direktiivin 2009/110/EY 5 artiklan 7 kohdan soveltamista, maksulaitosten ja sähköisen rahan liikkeeseenlaskijalaitosten tulee noudattaa näitä ohjeita yksilöllisellä tasolla.
11. Laitosten, maksulaitosten ja sähköisen rahan liikkeeseenlaskijalaitosten valvonnasta vastaavien toimivaltaisten viranomaisten tulee noudattaa näitä ohjeita.

Määritelmät

12. Ellei toisin määrätä, ohjeisiin sisältyvillä termeillä tarkoitetaan samaa kuin direktiivissä 2013/36/EU, asetuksessa (EU) N:o 575/2013, direktiivissä 2009/110/EY, direktiivissä (EU) 2015/2366 ja Euroopan pankkiviranomaisen ohjeissa hallinnosta ja ohjauksesta⁹ käytetyillä ja määritellyillä termeillä. Lisäksi näissä ohjeissa käytetään seuraavia määritelmiä:

Ulkoistaminen	tarkoittaa kaikentyypisiä laitoksen, maksulaitoksen tai sähköisen rahan liikkeeseenlaskijalaitoksen ja palveluntarjoajan välisiä järjestelyjä, joiden perusteella kyseinen palveluntarjoaja suorittaa sellaisen prosessin, palvelun tai toiminnan, jonka laitos, maksulaitos tai sähköisen rahan liikkeeseenlaskijalaitos olisi muuten itse suorittanut.
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

⁷ Euroopan parlamentin ja neuvoston direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta (EUVL L 173, 12.6.2014, s. 349).

⁸ Komission delegoitu asetukset (EU) 2017/565, annettu 25 päivänä huhtikuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU täydentämisestä sijoituspalveluyritysten toiminnan järjestämistä koskevien vaatimusten, toiminnan harjoittamisen edellytysten ja kyseisessä direktiivissä määriteltyjen käsitteiden osalta (EUVL L 87, 31.3.2017, s. 1).

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

Toiminto	tarkoittaa prosesseja, palveluja ja toimia.
Kriittinen tai tärkeä toiminto ¹⁰	tarkoittaa toimintoa, jonka katsotaan olevan kriittinen tai tärkeä näiden ohjeiden 4 jakson mukaisesti.
Edelleen ulkoistaminen	tarkoittaa tilannetta, jossa palveluntarjoaja ulkoistamisjärjestelyn puitteissa siirtää ulkoistetun toiminnon edelleen toiselle palveluntarjoajalle. ¹¹
Palveluntarjoaja	tarkoittaa kolmatta osapuolta, joka toteuttaa ulkoistetun prosessin, palvelun tai toimen tai osan siitä ulkoistamisjärjestelyn puitteissa.
Pilvipalvelut	tarkoittavat palveluja, joita tarjotaan tietotekniikan resurssipalvelujen avulla. Tämä tarkoittaa toimintamallia, joka mahdollistaa yleisesti saatavilla olevan, kätevän, tilattavan pääsyn vapaasti konfiguroitaviin tietotekniikkaresursseihin (esimerkiksi verkkoihin, palvelimiin, tallennustilaan, sovelluksiin ja palveluihin), joita voidaan hankkia ja ottaa käyttöön nopeasti siten, että hallinnointityö ja vuorovaikutus palveluntarjoajan kanssa ovat hyvin vähäisiä.
Julkiset pilvipalvelut	tarkoittavat avoimesti käytettävissä olevaa julkista pilvipalveluinfrastruktuuria.
Yksityiset pilvipalvelut	tarkoittavat yksinomaisesti yhden laitoksen tai maksulaitoksen käytettävissä olevaa pilvipalveluinfrastruktuuria.
Yhteisöpilvipalvelut	tarkoittavat pilvipalveluinfrastruktuuria, joka on yksinomaisesti tietyn laitosten tai maksulaitosten muodostaman yhteisön, kuten yhden konsernin useiden laitosten, käytettävissä.
Hybridipilvipalvelut	tarkoittavat kahdesta tai useammasta erillisestä pilvipalveluinfrastruktuurista koostuvaa pilvipalveluinfrastruktuuria.
Ylin hallintoelin	tarkoittaa laitoksen tai maksulaitoksen elintä tai elinten joukkoa, joka on nimitetty kansallisen lainsäädännön mukaisesti, jolla on valtuudet asettaa laitoksen tai maksulaitoksen strategia, tavoitteet ja yleinen suunta, joka valvoo ja seuraa johdon päätöksentekoa ja johon kuuluvat laitoksen tai maksulaitoksen liiketoimintaa

¹⁰ Sanamuoto ”kriittinen tai tärkeä toiminto” perustuu direktiivissä 2014/65/EU (MiFID II) ja MiFID II -direktiiviä täydentävässä komission delegoidussa asetuksessa (EU) 2017/565 käytettyyn sanamuotoon, ja sitä käytetään vain ulkoistamisen osalta; se ei liity direktiivin 2014/59/EU (pankkien elvytys- ja kriisinratkaisudirektiivi) 2 artiklan 1 kohdan 35 luetelmakohdassa annettuun ”kriittisten toimintojen” määritelmään elvytys- ja kriisinratkaisukehityksen yhteydessä.

¹¹ Arvioinnissa sovelletaan 3 jakson säännöksiä; edelleen ulkoistamiseen on viitattu muissa Euroopan pankkiviranomaisen asiakirjoissa myös ”ulkoistusketjuna” ja ”ketju-ulkoistamisena”.

tosiasiallisesti johtavat henkilöt sekä
maksulaitoksen johdosta vastaavat johtajat ja
henkilöt.

3. Täytäntöönpano

Soveltamispäivä

13. Näitä ohjeita sovelletaan 63 kohdan b alakohtaa lukuun ottamatta 30. syyskuuta 2019 alkaen kaikkiin ulkoistamisjärjestelyihin, jotka tehdään, arvioidaan tai joita muutetaan kyseisenä päivämääränä tai sen jälkeen. Ohjeiden 63 kohdan b alakohtaa sovelletaan 31. joulukuuta 2021 alkaen.
14. Laitosten ja maksulaitosten tulee arvioida nykyiset ulkoistamisjärjestelyt ja muutettava niitä tarpeen mukaan varmistaakseen, että ne ovat näiden ohjeiden mukaisia.
15. Jos kriittisiä tai tärkeitä toimintoja koskevia ulkoistamisjärjestelyjä ei ole arvioitu 31. joulukuuta 2021 mennessä, laitosten ja maksulaitosten tulee ilmoittaa tästä toimivaltaiselle viranomaiselle ja sisällytettävä ilmoitukseen suunnitellut toimenpiteet arvioinnin saattamiseksi päätökseen tai mahdollinen irtautumisstrategia.

Siirtymäsäännökset

16. Laitosten ja maksulaitosten tulee laatia kaikkia nykyisiä ulkoistamisjärjestelyjä (lukuun ottamatta pilvipalvelujen tarjoajien kanssa tehtyjä ulkoistamisjärjestelyjä) koskevat asiakirjat näiden ohjeiden mukaisesti kunkin nykyisen ulkoistamisjärjestelyn ensimmäisen uusimispäivämäärän jälkeen, kuitenkin viimeistään 31. joulukuuta 2021.

Kumoaminen

17. Euroopan pankkivalvontaviranomaisten komitean (CEBS) 14. joulukuuta 2006 antamat ulkoistamista koskevat ohjeet sekä Euroopan pankkiviranomaisen suositukset ulkoistamisesta pilvipalveluihin¹² kumotaan 30. syyskuuta 2019 alkaen.

¹² Suosituksia ulkoistamisesta pilvipalveluihin (EBA/REC/2017/03).

4. Ulkoistamista koskevat ohjeet

I osasto – suhteellisuus: ryhmät ja laitosten suojajärjestelmät

1 Suhteellisuus

18. Laitosten, maksulaitosten ja toimivaltaisten viranomaisten tulee soveltaa näiden ohjeiden noudattamiseen tai valvontaan suhteellisuusperiaatetta. Suhteellisuusperiaatteella pyritään varmistamaan, että ohjaus- ja hallintojärjestelmät, mukaan lukien ulkoistamiseen liittyvät järjestelmät, ovat yhdenmukaisia laitoksen tai maksulaitoksen yksilöllisen riskiprofiilin, luonteen ja liiketoimintamallin kanssa ja että toiminnan laajuus ja monimutkaisuus mahdollistavat sääntelyvaatimusten tehokkaan noudattamisen.
19. Kun näissä ohjeissa annettua vaatimuksia sovelletaan, laitosten ja maksulaitosten tulee huomioida ulkoistettujen toimintojen monimutkaisuus, ulkoistamisjärjestelystä koituvat riskit, ulkoistetun toiminnon kriittisyys tai tärkeys sekä ulkoistamisen mahdollinen vaikutus toiminnan jatkumiselle.
20. Laitosten, maksulaitosten ¹³ ja toimivaltaisten viranomaisten tulee huomioida suhteellisuusperiaatteen soveltamisessa kriteerit, jotka on määritetty Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden I osastossa direktiivin 2013/36/EU 74 artiklan 2 kohdan mukaisesti.

2 Laitosten suojajärjestelmään kuuluvien ryhmien ja laitosten ulkoistamistoimet

21. Direktiivin 2013/36/EU 109 artiklan 2 kohdan mukaisesti näitä ohjeita tulee soveltaa myös konsolidoidulla tasolla tai alakonsolidointiryhmän tasolla ja laitoksen vakavaraisuuteen kohdistuva konsolidointitulee huomioida.¹⁴ Tästä syystä EU:ssa emoyrityksenä toimivien tai jäsenvaltiossa emoyrityksenä toimivien laitostentulee varmistaa, että niiden tytäryhtiöiden, maksulaitokset mukaan lukien, sisäiset hallinto- ja ohjausjärjestelmät, -prosessit ja -mekanismit

¹³ Maksulaitosten on myös tarkastettava Euroopan pankkiviranomaisen uudistettua maksupalveludirektiiviä (PSD2) koskevista ohjeista, mitä tietoja on toimitettava maksulaitosten ja sähköisen rahan liikkeeseenlaskijalaitosten toimilupaa ja tilitietopalvelujen tarjoajien rekisteröintiä varten. Ohjeet ovat saatavilla Euroopan pankkiviranomaisen verkkosivustolla osoitteessa <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 Lisätietoa konsolidointiin soveltamisalasta on asetuksen (EU) N:o 575/2013 4 artiklan 1, 47 ja 48 kohdassa.

ovat johdonmukaisia, kiinteästi liitettyjä ja riittäviä, jotta näitä ohjeita voidaan soveltaa tehokkaasti kaikilla asianmukaisilla tasoilla.

22. 21 kohdan mukaisesti laitosten ja maksulaitosten sekä laitosten, jotka laitosten suojajärjestelmän jäseninä käyttävät keskitettyjä hallinto- ja ohjausjärjestelmiä, tulee täyttää seuraavat vaatimukset:

- a. kun laitoksilla tai maksulaitoksilla on ulkoistamisjärjestelyjä palveluntarjoajien kanssa ryhmän tai laitosten suojajärjestelmän¹⁵ sisällä, kyseisten laitosten tai maksulaitosten ylimmällä hallintoelimellä on täysi vastuu kaikkien sääntelyvaatimusten noudattamisesta ja näiden ohjeiden tehokkaasta soveltamista myös kyseisten ulkoistamisjärjestelyjen osalta
- b. kun laitokset tai maksulaitokset ulkoistavat sisäisen valvonnan operatiiviset tehtävät palveluntarjoajalle ryhmän tai laitosten suojajärjestelmän sisällä ulkoistamisjärjestelyiden valvonnan ja tarkastusten osalta, niidentulee varmistaa, että myös näihin ulkoistamisjärjestelyihin liittyvät operatiiviset tehtävät suoritetaan tehokkaasti, mukaan lukien asianmukaisten raporttien toimittaminen.

23. 22 kohdan lisäksi ryhmään kuuluvien laitosten ja maksulaitosten, joille ei ole myönnetty vapautusta direktiivin 2013/36/EU 109 artiklan ja asetuksen (EU) N:o 575/2013 7 artiklan nojalla, laitosten, jotka ovat keskuslaitoksia tai keskuslaitokseen pysyvästi liittyneitä laitoksia, joille ei ole myönnetty vapautusta direktiivin 2013/36/EU 21 artiklan nojalla, sekä laitosten suojajärjestelmään kuuluvien laitosten tulee huomioida seuraavat seikat:

- a. Kun ulkoistamisen operatiivinen seuranta on keskitetty (esim. osana ulkoistamisjärjestelyiden seurannan pääsopimusta), laitosten ja maksulaitosten tulee varmistaa, että palveluntarjoajan riippumaton seuranta ja jokaisen laitoksen tai maksulaitoksen asianmukainen valvonta on mahdollista vähintään kriittisten tai tärkeiden toimintojen osalta, mukaan lukien keskitetyltä seurantatoiminnolta vähintään vuosittain tai pyynnöstä saatavat raportit, jotka sisältävät vähintään riskinarviointin ja suorituskyvyn seurannan yhteenvedon. Lisäksi laitosten ja maksulaitosten tulee saada keskitetyltä seurantatoiminnolta yhteenveto asianmukaisista tarkastuskertomuksista, jotka koskevat kriittisiä tai tärkeitä ulkoistuksia, sekä pyydettyä täydellinen tarkastuskertomus.
- b. Laitosten ja maksulaitosten tulee varmistaa, että niiden ylimmälle hallintoelimelle ilmoitetaan asianmukaisesti oleellisista suunnitelluista muutoksista, jotka koskevat keskitetysti seurattuja palveluntarjoajia, sekä tällaisten muutosten mahdollisista vaikutuksista kriittisiin tai tärkeisiin toimintoihin, mukaan lukien riskianalyysin

¹⁵ Vakavaraisuusasetuksen 113 artiklan 7 kohdan mukaan laitosten suojajärjestelmä tarkoittaa sopimusperusteista tai lakisääteistä suojajärjestelmää, joka suojelee laitoksia ja tarvittaessa varmistaa ennen kaikkea niiden likviditeetin ja vakavaraisuuden konkurssin välttämiseksi.

yhteenvedo, oikeudelliset riskit, sääntelyvaatimusten noudattaminen ja vaikutus palvelutasoihin, jotta ne pystyvät arvioimaan kyseisten muutosten vaikutuksia.

- c. Kun ryhmän sisäisten laitosten tai maksulaitosten, keskuslaitokseen liittyneiden laitosten tai laitosten suojajärjestelmään kuuluvien laitosten ulkoistamisjärjestelyt on arvioitu ennen ulkoistamista keskitetysti 12 jakson mukaisesti, jokaisen laitoksen tai maksulaitoksen tulee saada yhteenvedo arvioinnista javarmistaa, että siinä huomioidaan sen erityisrakenne sekä päätöksentekoprosessin riskit.
 - d. Kun kaikista voimassa olevista ulkoistamisjärjestelyistä perustetaan rekisteri 11 jakson mukaisesti ja sitä ylläpidetään keskitetysti ryhmän tai laitosten suojajärjestelmän sisällä, toimivaltaisilla viranomaisilla sekä kaikilla laitoksilla ja maksulaitoksilla tulee olla pääsy rekisteriin ilman aiheetonta viivytystä. Rekisterin täytyy sisältää kaikki ulkoistamisjärjestelyt, mukaan lukien ulkoistamisjärjestelyt palveluntarjoajien kanssa kyseisen ryhmän tai laitosten suojajärjestelmän sisällä.
 - e. Kun laitoksilla tai maksulaitoksilla on kriittisiä tai tärkeitä toimintoja varten irtautumissuunnitelmat, jotka on laadittu ryhmätasolla, laitosten suojajärjestelmän tai keskuslaitoksen sisällä, kaikkien laitosten ja maksulaitosten tulee saada yhteenvedo suunnitelmasta javarmistaa, että suunnitelma voidaan toteuttaa tehokkaasti.
24. Kun vapautuksia on myönnetty direktiivin 2013/36/EU 21 artiklan nojalla tai direktiivin 2013/36/EU 109 artiklan 1 kohdan nojalla yhdessä asetuksen (EU) N:o 575/2013 7 artiklan kanssa, jäsenvaltiossa emoyrityksenä toimivan laitoksen tulee soveltaa näiden ohjeiden säännöksiä itseensä ja tytäryhtiöihinsä tai keskuslaitokseen ja siihen liittyneisiin laitoksiin kokonaisuutena.
25. Laitosten ja maksulaitosten, jotka ovat EU:ssa emoyrityksenä toimivien tai jäsenvaltiossa emoyrityksenä toimivien laitosten tytäryhtiöitä ja joille ei ole myönnetty vapautuksia direktiivin 2013/36/EU 21 artiklan nojalla tai direktiivin 2013/36/EU 109 artiklan 1 kohdan nojalla yhdessä asetuksen (EU) N:o 575/2013 7 artiklan kanssa, tulee varmistaa yksilöllisellä tasolla, että ne noudattavat näitä ohjeita.

II osasto – ulkoistamisjärjestelyiden arvioiminen

3 Ulkoistaminen

26. Laitosten ja maksulaitosten tulee määrittää, kuuluuko kolmannen osapuolen kanssa tehty järjestely ulkoistamisen määritelmän piiriin. Tässä arvioinnissa tulee huomioida, vastaako palveluntarjoaja sille ulkoistetusta toiminnosta (tai sen osasta) toistuvasti tai jatkuvasti ja kuuluisiko kyseinen toiminto (tai sen osa) tavanomaisesti toimintoihin, jotka laitos tai maksulaitos pystyy realistisesti hoitamaan itse, vaikka laitos tai maksulaitos ei olisi sitä aiemmin hoitanutkaan itse.

27. Kun palveluntarjoajan kanssa tehty järjestely kattaa useita toimintoja, laitosten ja maksulaitosten tulee huomioida arvioinnissa järjestelyn kaikki osa-alueet. Jos esimerkiksi tarjottuun palveluun sisältyy tallennuslaitteisto ja tietojen varmuuskopiointi, nämä tulee huomioida yhdessä.
28. Yleisperiaatteena on, että seuraavia ei pidetä laitosten ja maksulaitosten ulkoistettuina toimintoina:
- a. toiminnot, joissa laki vaatii käyttämään palveluntarjoajaa, kuten lakisääteinen tilintarkastus
 - b. markkinatietopalvelut (esim. Bloombergin, Moody'sin, Standard & Poor'sin ja Fitchin toimittamat tiedot)
 - c. maailmanlaajuiset verkkoinfrastruktuurit (esim. Visa ja MasterCard)
 - d. selvitys- ja toimitusjärjestelyt selvitysyhteisöjen, keskusvastapuolten sekä selvitysyhteisöjen ja niiden jäsenten välillä
 - e. maailmanlaajuiset rahaliikenteen sanomanvälityksen infrastruktuurit, jotka toimivat viranomaisten valvonnassa
 - f. kirjeenvaihtajapankkipalvelut
 - g. sellaisten palveluiden hankinta, joita laitos tai maksulaitos ei muussa tapauksessa hoitaisi itse (esim. arkkitehdin konsultointi, oikeudellisten lausuntojen antaminen ja edustaminen tuomioistuimessa ja hallintoelimissä, siivous, puutarhatyöt ja laitoksen tai maksulaitoksen tilojen kunnossapitotyöt, terveydenhoitopalvelut, yrityksen autojen huolto, pitopalvelu, automaattien huollot, toimistopalvelut, matkustuspalvelut, postituspalvelut, vastaanottovirkailijat, sihteerit ja puhelinvaihteen hoitajat), tai sellaisten tavaroiden (esim. muovikortit, kortinlukijat, toimistotarvikkeet, tietokoneet, kalusteet) tai hyödykkeiden (sähkö, kaasu, vesi, puhelinlinjat) hankinta.

4 Kriittiset tai tärkeät toiminnot

29. Laitosten ja maksulaitosten tulee aina pitää toimintoa kriittisenä tai tärkeänä seuraavissa tapauksissa:¹⁶
- a. kun siinä ilmenevä toimintahäiriö tai sen toteuttamatta jääminen heikentäisi oleellisesti seuraavia:

¹⁶ Katso myös 30 artikla komission delegoidussa asetuksessa (EU) N:o 2017/565, annettu 25 päivänä huhtikuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU täydentämisestä sijoituspalveluyritysten toiminnan järjestämisestä koskevien vaatimusten, toiminnan harjoittamisen edellytysten ja kyseisessä direktiivissä määriteltyjen käsitteiden osalta.

- i. toimilupavaatimusten tai muiden vaatimusten noudattaminen direktiivin 2013/36/EU, asetuksen (EU) N:o 575/2013, direktiivin 2014/65/EU, direktiivin (EU) 2015/2366 ja direktiivin 2009/110/EY sekä niiden sääntelyllisten velvoitteiden mukaisesti
 - ii. taloudellinen tulos
 - iii. pankki- ja maksupalveluiden ja -toimintojen vakavaraisuus ja jatkuvuus
- b. kun sisäisen valvonnan operatiiviset tehtävät on ulkoistettu, paitsi siinä tapauksessa, että arvioinnin mukaan ulkoistetun palvelun riittämättömällä tarjoamisella tai tarjoamatta jättämisellä ei olisi haitallista vaikutusta sisäisen valvonnan vaikuttavuuteen
 - c. kun ne aikovat ulkoistaa pankkitoimintoja tai maksupalveluita laajuudessa, joka edellyttää toimivaltaisen viranomaisen valtuutusta¹⁷ 12.1 jakson mukaisesti.

30. Jos kyseessä on laitos, toimintojen kriittisyyden tai tärkeyden arviointiin tulee kiinnittää erityistä huomiota, jos ulkoistaminen koskee ydinliiketoiminta-alueita ja kriittisiä toimintoja direktiivin 2014/59/EU¹⁸ 2 artiklan 1 kohdan 35 ja 36 alakohdan määritelmien sekä komission delegoidun asetuksen (EU) 2016/778¹⁹ 6 ja 7 artiklassa annettujen määräyksen liittyvien perusteiden mukaisesti. Toimintoja, jotka ovat välttämättömiä ydinliiketoiminta-alueiden tai kriittisten toimintojen kannalta, pidetään näissä ohjeissa kriittisinä tai tärkeinä toimintoina, paitsi siinä tapauksessa, että laitoksen arvioinnin mukaan ulkoistetun palvelun riittämättömällä tarjoamisella tai tarjoamatta jättämisellä ei olisi haitallista vaikutusta ydinliiketoiminta-alueen tai kriittisten toimintojen jatkuvuuteen.

31. Arvioidessaan, liittykö ulkoistamisjärjestely kriittiseen tai tärkeään toimintoon, laitosten ja maksulaitosten tulee huomioida 12.2 jaksossa kuvatun riskinarvioinnin tuloksen lisäksi vähintään seuraavat seikat:

- a. liittykö ulkoistamisjärjestely suoraan sellaisten pankkipalveluiden tai maksupalveluiden tarjoamiseen²⁰, joihin niillä on toimilupa

¹⁷ Katso direktiivin 2013/36/EU liitteessä I luetellut toimet.

¹⁸ Euroopan parlamentin ja neuvoston direktiivi 2014/59/EU, annettu 15 päivänä toukokuuta 2014, luottolaitosten ja sijoituspalveluyritysten elvytys- ja kriisinratkaisukehyksestä sekä neuvoston direktiivin 82/891/ETY, Euroopan parlamentin ja neuvoston direktiivien 2001/24/EY, 2002/47/EY, 2004/25/EY, 2005/56/EY, 2007/36/EY, 2011/35/EU, 2012/30/EU ja 2013/36/EU ja asetusten (EU) N:o 1093/2010 ja (EU) N:o 648/2012 muuttamisesta (pankkien elvytys- ja kriisinratkaisudirektiivi) (EUVL L 173, 12.6.2014, s. 190).

¹⁹ Komission delegoitu asetus (EU) 2016/778, annettu 2 päivänä helmikuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 2014/59/EU täydentämisestä niiden olosuhteiden ja edellytysten määrittelemiseksi, joiden täytyessä ylimääräisen rahoitusosuuden suorittamista jälkikäteen voidaan lykätä kokonaan tai osittain, ja perusteista, joiden mukaisesti määritetään kriittisten toimintojen sisältämä toiminta, palvelut ja toiminnot sekä ydinliiketoiminta-alueisiin sisältyvät liiketoiminta-alueet ja niihin liittyvät palvelut (EUVL L 131, 20.5.2016, s. 41).

²⁰ Katso direktiivin 2013/36/EU liitteessä I luetellut toimet.

- b. ulkoistetun toiminnon häiriöiden tai sen, että palveluntarjoaja jättää jatkuvasti tarjoamatta palvelua sovitulla palvelutasolla, mahdolliset vaikutukset seuraaviin:
 - i. lyhyt- ja pitkäaikaisen rahoituksen kestävyys ja taloudellinen elinkelpoisuus, mukaan lukien varat, pääoma, kustannukset, rahoitus, likviditeetti sekä tuotot ja tappiot
 - ii. liiketoiminnan jatkuvuus ja operatiivinen kestävyys
 - iii. operatiivinen riski, mukaan lukien menettelytapariskit, tieto- ja viestintätekniikkaan (ICT) liittyvät riskit ja oikeudelliset riskit
 - iv. maineriskit
 - v. tarvittaessa elvytys- ja kriisintarkaisusuunnittelu, kriisintarkaisukelpoisuus ja toiminnan jatkuvuus, kun tilanteeseen puututaan varhain, elvytys- tai kriisintarkaisutilanne
- c. ulkoistamisjärjestelyn mahdollinen vaikutus seuraavien toteuttamiseen:
 - i. kaikkien riskien tunnistaminen, seuraaminen ja hallinta
 - ii. kaikkien oikeudellisten ja sääntelyvaatimusten noudattaminen
 - iii. ulkoistetun toiminnon asianmukaisten tarkastusten toteuttaminen
- d. mahdollinen vaikutus asiakkaille tarjottuihin palveluihin
- e. kaikki ulkoistamisjärjestelyt, laitoksen tai maksulaitoksen riippuvuus samasta palveluntarjoajasta kokonaisuudessaan sekä samaan liiketoiminta-alueeseen kuuluvien ulkoistamisjärjestelyjen mahdollinen kumulatiivinen vaikutus
- f. ulkoistamisjärjestelyihin liittyvien liiketoiminta-alueiden koko ja monimutkaisuus
- g. mahdollisuus laajentaa ehdotettua ulkoistamisjärjestelyä ilman sopimuksen korvaamista tai tarkistamista
- h. mahdollisuus siirtää ehdotettu ulkoistamisjärjestely toiselle palveluntarjoajalle tarvittaessa tai haluttaessa sopimuksen ja käytännön näkökulmasta, mukaan lukien arvioidut riskit, liiketoiminnan jatkuvuuden heikentyminen, kustannukset ja aikakehys (korvattavuus)
- i. mahdollisuus palauttaa ulkoistettu toiminto takaisin laitokseen tai maksulaitokseen tarvittaessa tai haluttaessa
- j. tietosuoja ja salassapitovelvollisuuden rikkomisen tai tiedon saatavuutta tai eheyttä koskevan häiriön mahdollinen vaikutus laitokseen tai maksulaitokseen ja sen



asiakkaisiin, mukaan lukien esimerkiksi asetuksen (EU) 2016/679²¹ vaatimusten noudattaminen.

²¹ Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus).

III osasto – Hallintokehys

5 Luotettavat hallinnointi- ja ohjausjärjestelmät sekä kolmannen osapuolen muodostama riski

32. Osana sisäistä valvontajärjestelmää,²² sisäiset valvontamekanismit mukaan lukien,²³ laitoksilla ja maksulaitoksilla tulee olla kokonaisvaltainen koko laitosta koskeva riskienhallintajärjestelmä, joka kattaa kaikki liiketoiminnan osa-alueet ja sisäiset yksiköt. Kyseisellä järjestelmällä laitosten ja maksulaitosten tulee tunnistaa kaikki riskit, mukaan lukien kolmannen osapuolen kanssa tehtyjen järjestelyiden aiheuttamat riskit, ja hallita niitä. Riskienhallintajärjestelmän ansiosta laitosten ja maksulaitosten tulee pystyä tekemään tietoon perustuvia päätöksiä riskinotosta ja varmistamaan, että riskienhallintatoimia toteutetaan asianmukaisesti myös kyberriskien osalta.²⁴
33. Laitosten ja maksulaitosten tulee 1 jaksossa kuvatun suhteellisuusperiaatteen mukaisesti tunnistaa, arvioida, seurata ja hallita kaikkia kolmansien osapuolten kanssa tehtyjen järjestelyjen itselleen aiheuttamia tai mahdollisesti aiheuttamia riskejä huolimatta siitä, ovatko kyseiset järjestelyt ulkoistamisjärjestelyjä. Kaikkien kolmansien osapuolten kanssa tehtyjen järjestelyjen, mukaan lukien 26 ja 28 kohdissa kuvatut järjestelyt, aiheuttamat riskit ja erityisesti operatiiviset riskit tulee arvioida 12.2 jakson mukaisesti.
34. Laitosten ja maksulaitosten tulee varmistaa, että ne noudattavat kaikkia asetuksen (EU) 2016/679 vaatimuksia myös kolmansien osapuolten kanssa tehdyissä järjestelyissä ja ulkoistamisjärjestelyissä.

6 Luotettavat hallinnointi- ja ohjausjärjestelmät ja ulkoistaminen

35. Toimintojen ulkoistaminen ei voi johtaa ylimmän hallintoelimen velvollisuuksien delegoimiseen. Laitoksilla ja maksulaitoksilla on edelleen oltava täysi vastuu ja tilivelvollisuus kaikkien sääntelyllisten velvoitteiden noudattamisesta, mukana lukien kyky valvoa kriittisten tai tärkeiden toimintojen ulkoistamista.
36. Ylin hallintoelin on aina täysin vastuussa ja tilivelvollinen vähintään seuraavista seikoista:
- sen varmistaminen, että laitos tai maksulaitos täyttää jatkuvasti toimiluvan säilyttämisen ehdot, mukaan lukien toimivaltaisen viranomaisen mahdollisesti asettamat ehdot

²² Lisätietoa laitoksille on Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden V osastossa.

²³ Katso myös direktiivin 2015/2366 (uudistettu maksupalveludirektiivi) 11 artikla.

²⁴ Katso myös Euroopan pankkiviranomaisen ICT:n turvallisuusriskien hallintaa koskevat ohjeet (<https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management>) ja G7-maiden peruselementit kolmannen osapuolen aiheuttamien kyberturvallisuusriskien hallintaan rahoitusallalla (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

- b. laitoksen tai maksulaitoksen sisäinen organisaatio
 - c. eturistiriitojen tunnistaminen, arviointi ja hallinta
 - d. laitoksen tai maksulaitoksen strategioiden ja käytäntöjen määrittäminen (esim. liiketoimintamalli, riskinottohalu ja riskienhallintajärjestelmä)
 - e. laitoksen tai maksulaitoksen päivittäisen hallinnan valvominen, mukaan lukien kaikkien ulkoistamiseen liittyvien riskien hallinta
 - f. ylimmän hallintoelimen valvontatehtävä, mukaan lukien johdon päätöksenteon valvonta ja seuranta.
37. Ulkoistaminen ei saa vähentää sopivuusvaatimuksia, jotka koskevat laitoksen ylintä hallintoelintä, johtajia ja maksulaitoksen hallinnosta vastaavia henkilöitä sekä keskeisistä toiminnoista vastaavia henkilöitä. Laitoksilla ja maksulaitoksilla tulee olla asianmukainen pätevyys sekä riittävästi osaavaa henkilöstöä, jotta ulkoistamisjärjestelyjen asianmukainen hallinta ja valvonta voidaan varmistaa.
38. Laitosten ja maksulaitosten tulee tehdä seuraavat toimet:
- a. määritellä selkeästi vastuu ulkoistamisjärjestelyjen dokumentoinnista, hallinnasta ja valvonnasta
 - b. kohdentaa riittävästi resursseja, jotta kaikkia oikeudellisia ja sääntelyvaatimuksia voidaan noudattaa, mukaan lukien nämä ohjeet sekä kaikkien ulkoistamisjärjestelyiden dokumentointi ja seuranta
 - c. perustaa näiden ohjeiden 1 jakson mukaisesti ulkoistamistoiminto tai nimetä kokenut työntekijä, joka on suoraan vastuuvollinen ylimmälle hallintoelimelle (esim. valvontatoiminnon keskeisistä tehtävistä vastaava henkilö) ja vastaa ulkoistamisjärjestelyiden riskien hallinnasta ja valvonnasta osana laitoksen sisäistä valvontajärjestelmää sekä valvoo ulkoistamisjärjestelyiden dokumentointia. Pienten ja yksinkertaisten laitosten tai maksulaitosten tulee varmistaa vähintään johdon selkeä tehtävä- ja vastuunjako ulkoistamisjärjestelyiden seuranta ja valvontaa varten. Ulkoistamistoiminto voidaan osoittaa laitoksen tai maksulaitoksen ylimmän hallintoelimen jäsenelle.
39. Laitosten ja maksulaitosten tulee aina varmistaa toiminnan riittävä sisältö, jotta niistä ei tule pelkkiä ”tyhjiä kuoria” tai postilaatikkoyhteisöjä. Tätä varten niiden tulee täyttää seuraavat ehdot:

- a. Toimiluvan ehtoja²⁵ tulee ainanoudattaa, ja ylimmän hallintoelimen tulee hoitaa tehokkaasti näiden ohjeiden 36 määritetyt velvollisuutensa.
- b. Selkeä ja läpinäkyvä organisaatiokehys ja -rakennetulee säilyttää, jotta oikeudellisia ja sääntelyvaatimuksia voidaan noudattaa.
- c. Jos sisäisen valvonnan operatiiviset tehtävät on ulkoistettu (esim. ryhmäsisäinen ulkoistaminen tai laitosten suojajärjestelmän sisäinen ulkoistaminen), asianmukainen valvonta tulee varmistaa ja kriittisten tai tärkeiden toimintojen ulkoistamisesta johtuvia riskejä tulee pystyä hallitsemaan.
- d. Kohdissa (a)–(c) esitettyjen vaatimusten noudattaminen tulee varmistaa riittäväillä resursseilla ja valmiuksilla.

40. Ulkoistamisen yhteydessä laitosten ja maksulaitosten tulee varmistaa vähintään seuraavat seikat:

- a. Laitokset tai maksulaitokset pystyvät tekemään ja toteuttamaan liiketoimintaan sekä kriittisiin tai tärkeisiin toimintoihin liittyviä päätöksiä, mukaan lukien ulkoistettuja toimintoja koskevat päätökset.
- b. Liiketoiminta sekä tarjottavat pankki- ja maksupalvelut säilyvät suunnitelmallisina.
- c. Senhetkisiin ja suunniteltuihin ulkoistamisjärjestelyihin liittyvät riskit, tieto- ja viestintätekniikkaan (ICT) sekä finanssiteknologiaan (Fintech) liittyvät riskit mukaan lukien, tunnistetaan ja arvioidaan ja niitä hallitaan ja vähennetään asianmukaisesti.
- d. Asianmukaiset tietojen salassapitoa koskevat järjestelyt ovat olemassa.
- e. Oleellisten tietojen sujuva tiedonkulku palveluntarjoajillelläpidetään.
- f. Kun kyseessä on kriittisten tai tärkeiden toimintojen ulkoistaminen, laitosten tulee pystyä tekemään vähintään yksi seuraavista toimista asianmukaisessa ajassa:
 - i. siirtämään toiminto vaihtoehtoiselle palveluntarjoajalle
 - ii. palauttamaan toiminto takaisin laitokselle

²⁵ Katso myös direktiivin 2013/36/EU 8 artiklan 2 kohta, joka koskee teknisiä sääntelystandardeja toimivaltaisille viranomaisille luottolaitosten toimilupahakemuksissa toimitettavista tiedoista, ja direktiivin 2013/36/EU 8 artiklan 3 kohta, joka koskee teknisiä täytäntöönpanostandardeja vakiomuotoisista lomakkeista, malleista ja menettelyistä luottolaitosten toimilupahakemuksissa toimitettavia tietoja varten (<https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions>).

Euroopan pankkiviranomaisen direktiiviä (EU) 2015/2366 (uudistettu maksupalveludirektiivi) koskevissa ohjeissa on maksulaitoksille lisätietoa siitä, mitä tietoja on toimitettava maksulaitosten ja sähköisen rahan liikkeeseenlaskijalaitosten toimilupaa ja tilitietopalvelujen tarjoajien rekisteröintiä varten (<https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf>).

iii. keskeyttämään toiminnosta riippuvat liiketoimet.

- g. Kun EU:hun ja/tai kolmansiin maihin sijoittautuneet palveluntarjoajat käsittelevät henkilötietoja, asianmukaiset toimet tulee toteuttaa ja tietoja tulee käsitellä asetuksen (EU) 2016/679 mukaisesti.

7 Ulkoistamisperiaatteet

41. Laitoksen tai maksulaitoksen, jolla on ulkoistamisjärjestelyjä tai joka aikoo toteuttaa tällaisia järjestelyjä, ylimmän hallintoelimen²⁶ tulee hyväksyä, tarkastaa säännöllisesti ja päivittää kirjalliset ulkoistamisperiaatteet jävarmistaa, että niitä noudatetaan yksilöllisellä, konsolidoidulla ja alakonsolidointiryhmän tasolla. Laitosten ulkoistamisperiaatteiden tulee vastata Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden 8 jaksoa, ja niissä tulee huomioida erityisesti ohjeiden 18 jaksossa esitetyt vaatimukset (Uudet tuotteet ja merkittävät muutokset). Maksulaitokset voivat myös linjata käytäntönsä Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden 8 ja 18 jakson mukaisesti.
42. Käytännössä tulee määritellä ulkoistamisjärjestelyiden elinkaaren päävaiheet sekä ulkoistamiseen liittyvät periaatteet, vastuut ja prosessit. Periaatteiden tulee kattaa vähintään seuraavat seikat:
- a. ylimmän hallintoelimen vastuut 36 kohdan mukaisesti, mukaan lukien osallistuminen ulkoistettuja kriittisiä tai tärkeitä toimintoja koskevaan päätöksentekoon tarvittaessa
 - b. liiketoiminnan osa-alueiden, sisäisen valvontatoiminnon ja muiden henkilöiden osallistuminen ulkoistamisjärjestelyihin
 - c. ulkoistamisjärjestelyiden suunnitteleminen, mukaan lukien seuraavat seikat:
 - i. ulkoistamisjärjestelyjä koskevien liiketoiminnan vaatimusten määrittäminen
 - ii. kriteerit, mukaan lukien 4 jaksossa luetellut kriteerit, ja prosessit kriittisten tai tärkeiden toimintojen tunnistamista varten
 - iii. riskien tunnistaminen, arviointi ja hallinta 12.2 jakson mukaisesti
 - iv. mahdollisten palveluntarjoajien due diligence -tarkastus, mukaan lukien 12.3 jaksossa kuvatut toimet
 - v. menettelyt mahdollisten eturistiriitojen tunnistamista, arviointia, hallintaa ja vähentämistä varten 8 jakson mukaisesti

²⁶ Katso myös Euroopan pankkiviranomaisen ohjeet maksupalvelujen operatiivisia riskejä ja turvallisuusriskejä koskevista turvatoimenpiteistä direktiivin (EU) 2015/2366 (PSD2) mukaisesti. Se on saatavilla osoitteessa <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>

- vi. liiketoiminnan jatkuvuutta koskevat suunnitelmat 9 jakson mukaisesti
 - vii. uusien ulkoistamisjärjestelyiden hyväksymisprosessi
- d. ulkoistamisjärjestelyiden toteuttaminen, seuranta ja hallinta, mukaan lukien seuraavat seikat:
- i. palveluntarjoajan toiminnan jatkuva arviointi 14 jakson mukaisesti
 - ii. menettelyt ulkoistamisjärjestelyyn tai palveluntarjoajaan liittyvistä muutoksista (esim. taloudellisen tilanteen, organisaatio- tai omistajarakenteiden tai edelleen ulkoistamisen muutoksista) ilmoittamista ja niihin reagoimista varten
 - iii. oikeudellisten ja sääntelyvaatimusten noudattamisen riippumaton arviointi ja tarkastus
 - iv. uusimisprosessit
- e. dokumentointi ja arkistointi, huomioiden 11 jakson vaatimukset
- f. irtautumisstrategiat ja keskeyttämisprosessit, ja jos ulkoistamisen keskeyttämistä pidetään mahdollisena, jokaiselle ulkoistettavalle kriittiselle tai tärkeälle toiminnolle tulee laatia lisäksi dokumentoitu irtautumisstrategia, jossa huomioidaan mahdolliset palvelukatkokset ja ulkoistamissopimuksen äkillinen päättyminen.
43. Ulkoistamisperiaatteissa tulee erottaa seuraavat seikat toisistaan:
- a. kriittisten tai tärkeiden toimintojen ulkoistaminen ja muut ulkoistamisjärjestelyt
 - b. ulkoistaminen palveluntarjoajille, joilla on toimivaltaisen viranomaisen myöntämä toimilupa, ja palveluntarjoajille, joilla ei ole toimilupaa
 - c. ryhmän sisäiset ulkoistamisjärjestelyt, laitosten suojajärjestelmän sisäiset ulkoistamisjärjestelyt (mukaan lukien laitosten suojajärjestelmään kuuluvien yritysten yksittäin tai yhdessä kokonaan omistamat yksiköt) sekä ryhmän ulkoiset ulkoistamisjärjestelyt
 - d. ulkoistaminen palveluntarjoajille, jotka ovat sijoittautuneet jäsenvaltioon, ja palveluntarjoajille, jotka ovat sijoittautuneet kolmansiin maihin.
44. Laitosten ja maksulaitosten tulee varmistaa, että käytännöt kattavat seuraavien kriittisten tai tärkeiden ulkoistamisjärjestelyjen mahdollisten vaikutusten tunnistamisen ja että nämä vaikutukset huomioidaan päätöksentekoprosessissa:
- a. laitoksen riskiprofiili
 - b. kyky valvoa palveluntarjoajaa ja hallita riskejä

- c. liiketoiminnan jatkuvuuteen liittyvät toimet
- d. muiden liiketoimien suorituskyky.

8 Eturistiriidat

45. Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden IV osaston 11 jakson mukaan laitosten ²⁷ ja maksulaitosten tulee tunnistaa, arvioida ja hallita ulkoistamisjärjestelyihin liittyviä eturistiriitoja.
46. Jos ulkoistaminen synnyttää oleellisen eturistiriidan samaan ryhmään tai laitosten suojajärjestelmään kuuluvien yritysten välillä, laitosten ja maksulaitosten tulee ryhtyä asianmukaisiin toimenpiteisiin, joilla eturistiriitoja voidaan hallita.
47. Kun toiminnot tarjoaa palveluntarjoaja, joka kuuluu ryhmään tai laitosten suojajärjestelmään tai jonka omistaa laitos, maksulaitos, ryhmä tai laitokset, jotka kuuluvat samaan laitosten suojajärjestelmään, ulkoistettua palvelua koskevat edellytykset, rahoitukselliset edellytykset mukaan lukien, tulee pitää riittävän erillään. Palveluiden hinnoittelussa voidaan kuitenkin huomioida syntyvät synergiat, kun samoja tai samankaltaisia palveluita tarjotaan useille laitoksille ryhmän tai laitosten suojajärjestelmän sisällä, edellyttäen, että palveluntarjoaja pysyy yksinään elinkelpoisena. Ryhmän sisällä tämä tarkoittaa riippumattomuutta ryhmän muiden laitosten konkurseista.

9 Liiketoiminnan jatkuvuutta koskevat suunnitelmat

48. Direktiivin 2013/36/EU 85 artiklan 2 kohdan ja Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden²⁸ VI osaston mukaisesti laitoksilla ja maksulaitoksilla tulee olla käytössä ulkoistettujen kriittisten tai tärkeiden toimintojen asianmukaiset liiketoiminnan jatkuvuutta koskevat suunnitelmat, joita tulee ylläpitää ja testata säännöllisesti. Ryhmään tai laitosten suojajärjestelmään kuuluvilla laitoksilla tai maksulaitoksilla voi olla keskitetty liiketoiminnan jatkuvuutta koskeva suunnitelma ulkoistettuja toimintoja varten.
49. Liiketoiminnan jatkuvuutta koskevissa suunnitelmassa tulee huomioida se mahdollisuus, että ulkoistetun kriittisen tai tärkeän toiminnon laatu laskee tasolle, jota ei voida pitää hyväksyttävänä, tai että palveluntarjoaja ei kykene tarjoamaan palvelua. Tällaisissa suunnitelmissa tulee huomioida myös maksukyvyttömyyden tai palveluntarjoajien laiminlyöntien vaikutukset sekä mahdolliset poliittiset riskit palveluntarjoajan oikeudenkäyttöalueella.

²⁷ Maksulaitosten käytännöt voivat myös noudattaa näitä ohjeita.

²⁸ Saatavilla osoitteessa <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->

10 Sisäinen tarkastustoiminto

50. Sisäisen tarkastustoiminnon²⁹ tehtäviin kuuluu ulkoistettujen palveluiden riippumaton tarkastus riskiperusteisen lähestymistavan mukaisesti. Tarkastussuunnitelmaan³⁰ ja -ohjelmaan tulee sisältyä erityisesti kriittisten tai tärkeiden toimintojen ulkoistamisjärjestelyt.
51. Ulkoistamisprosessin osalta sisäisen tarkastustoiminnon tulee varmistaa vähintään seuraavat seikat:
- laitoksen tai maksulaitoksen ulkoistamiskehystä, periaatteet mukaan lukien, sovelletaan oikein ja tehokkaasti, ja se on sovellettavien lakien ja asetusten, riskistrategian ja ylimmän hallintoelimen päätösten mukainen
 - toimintojen kriittisyys tai tärkeys arvioidaan riittävällä, laadukkaalla ja tehokkaalla tavalla
 - ulkoistamisjärjestelyiden riskinarviointi tehdään riittävällä, laadukkaalla ja tehokkaalla tavalla, ja riskit pysyvät laitoksen riskistrategiassa määritetyissä rajoissa
 - hallintoelimet osallistuvat asianmukaisesti
 - ulkoistamisjärjestelyiden seuranta ja hallinta on asianmukaista.

11 Dokumentointivaatimukset

52. Laitosten ja maksulaitosten tulee ylläpitää osana riskienhallintajärjestelmäänsä ajantasaista rekisteriä kaikista ulkoistamisjärjestelyistä laitoksen tasolla ja tarvittaessa konsolidoidulla ja alakonsolidointiryhmän tasolla 2 jakson mukaisesti. Kaikki voimassa olevat ulkoistamisjärjestelyt tulee dokumentoida asianmukaisesti, ja kriittisten tai tärkeiden toimintojen ulkoistaminen ja muut ulkoistamisjärjestelyt on erotettava toisistaan. Laitosten on säilytettävä päätyneitä ulkoistamisjärjestelyitä koskevat tiedot ja täydentävät asiakirjat rekisterissä asianmukaisen pituisen ajan. Tässä tulee huomioida kansallinen lainsäädäntö.
53. Rekisteriä voidaan pitää keskitetysti. Tässä tulee huomioida näiden ohjeiden I osasto sekä 23 kohdan d alakohdassa esitetyt ehdot, jos kyseessä on ryhmään kuuluva laitos tai maksulaitos, keskuslaitokseen pysyvästi liittyneet laitokset tai samaan laitosten suojajärjestelmään kuuluvat laitokset.

²⁹ Laitokset saavat lisätietoa sisäisen tarkastustoiminnon velvollisuuksista Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden 22 jaksosta (<https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->) ja maksulaitokset Euroopan pankkiviranomaisen maksulaitosten toimilupaa koskevien ohjeiden ohjeesta 5
(<https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf>).

³⁰ Katso myös Euroopan pankkiviranomaisen valvojan arviointiprosessia (SREP) koskevat ohjeet: <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>

54. Rekisterissä tulee olla vähintään seuraavat tiedot kaikista voimassa olevista ulkoistamisjärjestelyistä:

- a. kunkin ulkoistamisjärjestelyn viitenumero
- b. alkamispäivä ja tarvittaessa sopimuksen seuraava uusimispäivä, päättymispäivä ja/tai palveluntarjoajaa ja laitosta tai maksulaitosta koskevat irtisanomisajat
- c. ulkoistetun toiminnon lyhyt kuvaus, mukaan lukien ulkoistetut tiedot ja tieto siitä (esimerkiksi vastaamalla kyllä tai ei erillisessä tietokentässä), onko henkilötietoja siirretty tai onko niiden käsittely ulkoistettu palveluntarjoajalle
- d. laitoksen tai maksulaitoksen määrittämä luokka, joka kuvaa toiminnon luonnetta kohdan (c) mukaisesti (esim. tietotekniikka, valvontatoiminto) ja helpottaa erilaisten järjestelytyyppien tunnistamista
- e. palveluntarjoajan nimi, yrityksen rekisteröintinumero, oikeushenkilötunnus (jos saatavissa), rekisteröity osoite ja muut oleelliset yhteystiedot sekä mahdollisen emoyhtiön nimi
- f. maa tai maat, joissa palvelu toteutetaan, mukaan lukien tietojen sijainti (maa tai alue)
- g. tieto siitä (kyllä/ei), pidetäänkö ulkoistettua toimintoa kriittisenä tai tärkeänä, mukaan lukien tarvittaessa lyhyt yhteenveto perusteista, joiden nojalla ulkoistettua toimintoa pidetään kriittisenä tai tärkeänä
- h. jos kyseessä on ulkoistaminen pilvipalvelujen tarjoajalle, pilvipalvelun malli ja pilvipalvelun käytön malli eli se, onko pilvipalvelu julkinen/yksityinen/hybridi/yhteisö, sekä säilytettävien tietojen täsmällinen luonne ja sijainnit (esim. maat tai alueet), joissa tällaisia tietoja säilytetään
- i. kriittisen tai tärkeän ulkoistetun toiminnon viimeisimmän arvioinnin päivämäärä.

55. Ulkoistetuista kriittisistä tai tärkeistä toiminnoista rekisteriin on lisättävä vähintään seuraavat tiedot:

- a. mahdolliset varovaisuusperiaatteen mukaisen konsolidoinnin piiriin tai laitosten suojajärjestelmään kuuluvat laitokset, maksulaitokset tai muut yritykset, jotka hyödyntävät ulkoistusta
- b. tieto siitä, onko palveluntarjoaja tai alihankintana toimitettavien palvelujen toimittaja ryhmän tai laitosten suojajärjestelmän jäsen tai omistavatko sen ryhmään kuuluvat laitokset tai maksulaitokset tai laitosten suojajärjestelmän jäsenet
- c. uusimman riskinarvioinnin päivämäärä ja lyhyt yhteenveto sen tuloksista

- d. laitoksen tai maksulaitoksen työntekijä tai päätöksentekoelein (esim. ylin hallintoelin), joka hyväksyi ulkoistamisjärjestelyn
 - e. ulkoistamisjärjestelyä säätelevä laki
 - f. uusimman ja seuraavien sovittujen tarkastusten päivämäärät tarvittaessa
 - g. mahdollisten sellaisten alihankkijoiden nimet, joille kriittisten tai tärkeiden toimintojen oleelliset osat on ulkoistettu edelleen, mukaan lukien maa, jossa alihankkijat ovat rekisteröityneet ja jossa palvelu toteutetaan sekä tarvittaessa tietojen tallennussijainti (maa tai alue)
 - h. palveluntarjoajan korvattavuutta koskevan arvioinnin tulos (eli onko korvaaminen helppoa, vaikeaa tai mahdotonta), mahdollisuus palauttaa kriittiset tai tärkeät toiminnot laitoksen tai maksulaitoksen sisälle tai kriittisen tai tärkeän toiminnon keskeyttämisen vaikutukset
 - i. vaihtoehtoisten palveluntarjoajien tunnistaminen kohdan (h) mukaisesti
 - j. tieto siitä, tukeeko ulkoistettu kriittinen tai tärkeä toiminto aikakriittistä liiketoimintaa
 - k. arvioidut vuotuiset budjetoidut kustannukset.
56. Laitosten tai maksulaitosten on toimitettava pyynnöstä toimivaltaiselle viranomaiselle joko koko voimassa olevia ulkoistamisjärjestelyjä koskeva rekisteri³¹ tai sen määritetyt osat, kuten tiedot kaikista ulkoistamisjärjestelyistä, jotka kuuluvat johonkin näiden ohjeiden 54 kohdan (d) alakohdassa tarkoitettuihin luokkiin (esim. kaikki tietotekniikan ulkoistamisjärjestelyt). Laitosten tai maksulaitosten on toimitettava nämä tiedot muokattavassa sähköisessä muodossa (esim. yleinen tietokantamuoto, CSV)
57. Laitosten ja maksulaitosten on toimitettava toimivaltaiselle viranomaiselle pyynnöstä kaikki tarvittavat tiedot, mukaan lukien tarvittaessa ulkoistamissopimuksen kopio, jotta toimivaltainen viranomainen pystyy valvomaan laitosta tai maksulaitosta tehokkaasti.
58. Laitosten ja, rajoittamatta kuitenkaan direktiivin (EU) 2015/2366 19 artiklan 6 kohdan soveltamista, maksulaitosten on ilmoitettava asianmukaisesti ja hyvissä ajoin toimivaltaisille viranomaisille tai käytävä vuoropuhelua toimivaltaisen valvontaviranomaisen kanssa kriittisten tai tärkeiden toimintojen suunnitellusta ulkoistamisesta ja/tai ulkoistetun toiminnon muuttumisesta kriittiseksi tai tärkeäksi ja toimitettava vähintään 54 kohdassa esitetyt tiedot.

³¹ Katso myös Euroopan pankkiviranomaisen valvojan arviointiprosessia (SREP) koskevat ohjeet. Ne ovat saatavissa osoitteessa <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2>

59. Laitosten ja maksulaitosten³² on ilmoitettava toimivaltaisille viranomaisille hyvissä ajoin ulkoistamisjärjestelyidensä oleellisista muutoksista ja/tai niihin liittyvistä vakavista tapahtumista, jotka voivat vaikuttaa oleellisesti laitosten tai maksulaitosten liiketoiminnan jatkuvuuteen.
60. Laitosten ja maksulaitosten tulee dokumentoida asianmukaisesti IV osaston mukaiset arvioinnit ja jatkuvan valvonnan tulokset (esim. palveluntarjoajan suorituskyky, sovittujen palvelutasojen noudattaminen, muut sopimusvelvoitteet ja sääntelyvaatimukset, riskinarvioinnin päivitykset).

IV osasto – ulkoistamisprosessi

12 Ulkoistamista edeltävä analyysi

61. Ennen minkään ulkoistamisjärjestelyn toteuttamista laitosten ja maksulaitosten tulee tehdä seuraavat toimet:
- arvioida II osaston mukaisesti, koskeeko ulkoistamisjärjestely kriittistä tai tärkeää toimintoa
 - arvioida, täyttyvätkö 12.1 jaksossa esitetyt valvontaa koskevat ehdot
 - tunnistaa kaikki ulkoistamisjärjestelyyn liittyvät oleelliset riskit 12.2 jakson mukaisesti
 - tehdä mahdollisen palveluntarjoajan due diligence -tarkastus 12.3 jakson mukaisesti
 - tunnistaa ja arvioida ulkoistamiseen mahdollisesti liittyvät eturistiriidat 8 jakson mukaisesti.

12.1 Valvontaa koskevat ehdot

62. Jos pankkitoimintaa³³ tai maksupalveluita ulkoistetaan samaan tai toiseen jäsenvaltioon sijoittautuneelle palveluntarjoajalle siinä laajuudessa, että toiminnon suorittaminen edellyttää toimivaltaisen viranomaisen myöntämää toimilupaa tai rekisteröintiä siinä jäsenvaltiossa, jossa niillä on toimilupa, laitosten ja maksulaitosten tulee varmistaa, että jokin seuraavista ehdoista täyttyy:
- toimivaltainen viranomainen on myöntänyt palveluntarjoajalle toimiluvan tai rekisteröinyt sen kyseistä pankkitoimintaa tai maksupalveluita varten

³² Katso myös Euroopan pankkiviranomaisen ohjeet direktiivin (EU) 2015/2366 (PSD2) mukaisesta merkittävien häiriöiden raportoinnista osoitteessa <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>

³³ Katso vakavaraisuusdirektiivin 9 artikla, joka koskee muita henkilöitä tai yrityksiä kuin luottolaitoksia koskevaa kieltoa vastaanottaa yleisöltä talletuksia tai muita takaisin maksettavia varoja.

- b. palveluntarjoajalla on muuten lupa kyseiselle pankkitoiminnalle tai maksupalveluille kansallisen oikeudellisen kehyksen nojalla.

63. Jos pankkitoimintaa tai maksupalveluita ulkoistetaan kolmanteen maahan sijoittautuneelle palveluntarjoajalle siinä laajuudessa, että toiminnon suorittaminen edellyttää toimivaltaisen viranomaisen myöntämää toimilupaa tai rekisteröintiä siinä jäsenvaltioissa, jossa niillä on toimilupa, laitosten ja maksulaitosten tulee varmistaa, että seuraavat ehdot täyttyvät:

- a. palveluntarjoajalla on toimilupa tai se on rekisteröity kyseistä pankkitoimintaa tai maksupalvelua varten kolmannessa maassa ja sen toimintaa valvoo kyseisen kolmannen maan asianomainen toimivaltainen viranomainen (valvontaviranomainen)
- b. laitoksen valvonnasta vastaavat toimivaltaiset viranomaiset ja palveluntarjoajan valvonnasta vastaavat valvontaviranomaiset ovat solmineet asianmukaisen yhteistyösopimuksen, kuten aiesopimuksen tai kollegiosopimuksen
- c. kohdassa (b) tarkoitettulla yhteistyösopimuksella tulee varmistaa, että toimivaltaiset viranomaiset pystyvät vähintään
 - i. saamaan pyynnöstä tarvittavat tiedot, jotta ne voivat hoitaa direktiivin 2013/36/EU, asetuksen (EU) N:o 575/2013, direktiivin (EU) 2015/2366 ja direktiivin 2009/110/EY mukaiset valvontatehtävänsä
 - ii. tutustumaan kolmannessa maassa olevien valvontatehtäviensä hoidon kannalta merkityksellisiin tietoihin, asiakirjoihin, tiloihin tai henkilöstöön
 - iii. saamaan tietoa kolmannen maan valvontaviranomaiselta niin pian kuin mahdollista direktiivin 2013/36/EU, asetuksen (EU) N:o 575/2013, direktiivin (EU) 2015/2366 ja direktiivin 2009/110/EY mukaisten vaatimusten selvien rikkomisten tutkimista varten
 - iv. tekemään täytäntöönpanoon liittyvää yhteistyötä kolmannen maan valvontaviranomaisten kanssa, jos sovellettavia sääntelyvaatimuksia ja jäsenvaltion kansallista lakia on rikottu. Yhteistyöhön täytyy kuulua vähintään se, että kolmannen maan valvontaviranomaiset toimittavat tietoa sovellettavien sääntelyvaatimusten mahdollisista rikkomuksista niin pian kuin käytännössä on mahdollista.

12.2 Ulkoistamisjärjestelyiden riskinarviointi

64. Laitosten ja maksulaitosten tulee arvioida ulkoistamisjärjestelyiden mahdollinen vaikutus operatiiviseen riskiin, huomioida tämän arvioinnin tulokset päättäessään toiminnon ulkoistamisesta palveluntarjoajalle ja ryhtyä ennen ulkoistamisjärjestelyjen toteuttamista tarvittaviin toimiin, jotta operatiivisten riskien tarpeeton kasvu voidaan välttää.

65. Arvioinnissa tulee tarvittaessa tarkastella mahdollisia riskiskenaarioita, mukaan lukien vakavien tapahtumien aiheuttamat operatiivinen riski. Laitosten ja maksulaitosten tulee tarkastella skenaarioanalyysissä epäonnistuneiden tai riittämättömien palveluiden mahdollista vaikutusta, mukaan lukien prosessien, järjestelmien, ihmisten tai ulkoisten tapahtumien aiheuttamat riskit. Laitosten ja maksulaitosten tulee dokumentoida tehdyt analyysit ja niiden tulokset 1 jaksossa tarkoitetun suhteellisuusperiaatteen mukaisesti jaarvioida, miten paljon ulkoistamisjärjestely suurentaa tai pienentää operatiivista riskiä. I osaston mukaisesti pienet ja yksinkertaiset laitokset ja maksulaitokset voivat käyttää kvalitatiivisia riskinarviointimenetelmiä, kun taas suurten ja monimutkaisten laitosten tulee soveltaa edistyneempää menetelmää ja käytettävä sisäisiä ja ulkoisia tappiotietoja skenaarioanalyysissä, jos tiedot ovat saatavissa.
66. Laitosten ja maksulaitosten tulee huomioida riskinarvioinnissa ehdotetun ulkoistamisjärjestelyn odotetut hyödyt ja kustannukset, ja punnita mahdollisesti pieneneviä tai paremmin hallinnassa olevia riskejä sekä ehdotetusta ulkoistamisjärjestelystä mahdollisesti koituvia riskejä. Vähintään seuraavat seikat tulee huomioida:
- a. keskittämiskit, joiden syinä voivat olla seuraavat seikat:
 - i. ulkoistaminen vallitsevassa asemassa olevalle palveluntarjoajalle, joka ei ole helposti korvattavasti
 - ii. useat ulkoistamisjärjestelyt samalle palveluntarjoajalle tai toisiinsa kytköksissä oleville palveluntarjoajille
 - b. kokonaisriski, joka johtuu laitoksen tai maksulaitoksen useiden toimintojen ulkoistamisesta, tai jos kyseessä on laitosten ryhmä tai laitosten suojajärjestelmä, kokonaisriski konsolidoidulla tasolla tai laitosten suojajärjestelmän tasolla
 - c. jos kyseessä on merkittävä laitos, riski siitä, että laitoksen täytyy puuttua palveluntarjoajan toimintaan esimerkiksi antamalla taloudellista tukea ahdingossa olevalle palveluntarjoajalle tai ottamalla sen liiketoiminnan vastuulle
 - d. laitoksen tai maksulaitoksen ja palveluntarjoajan toteuttamat riskien hallintaan ja pienentämiseen tähtäävät toimet.
67. Jos ulkoistamisjärjestelyyn sisältyy sellainen mahdollisuus, että palveluntarjoaja voi ulkoistaa kriittisiä tai tärkeitä toimintoja edelleen muille palveluntarjoajille, laitosten ja maksulaitosten tulee huomioida seuraavat seikat:
- a. edelleen ulkoistamiseen liittyvät riskit, mukaan lukien riskit, joita voi koitua, jos alihankkija on sijoittautunut kolmanteen maahan tai eri maahan kuin palveluntarjoaja
 - b. riski siitä, että pitkä ja monimutkainen edelleenulkoistusketju heikentää laitosten tai maksulaitosten kykyä valvoa ulkoistettua kriittistä tai tärkeää toimintoa sekä toimivaltaisten viranomaisten tehokasta valvontaa.

68. Kun laitokset ja maksulaitokset tekevät riskinarviointia ennen ulkoistamista ja palveluntarjoajan suorituskyvyn jatkuvan tarkkailun aikana, niiden tulee tehdä vähintään seuraavat toimet:

- a. määrittää ja luokitella oleelliset toimet sekä niihin liittyvät tiedot ja järjestelmät arkaluonteisuuden ja vaadittujen turvatoimien mukaan
- b. tehdä perusteellinen riskinarviointi toiminnoille sekä niihin liittyville tiedoille ja järjestelmille, joiden ulkoistamista harkitaan tai jotka on ulkoistettu, ja huomioida mahdolliset riskit ja etenkin operatiiviset riskit, mukaan lukien oikeudelliset riskit, tieto- ja viestintätekniikkaan liittyvät riskit, vaatimustenmukaisuuteen liittyvät riskit ja maineriskit, sekä valvontaan liittyvät rajoitteet maissa, joissa ulkoistetut palvelut toteutetaan tai joissa niitä voidaan tarjota, sekä maissa, joissa tiedot sijaitsevat tai joissa tietoja todennäköisesti säilytetään
- c. huomioida palveluntarjoajan sijainnin (EU:n sisällä tai ulkopuolella) mahdolliset vaikutukset
- d. huomioida kyseisten oikeudenkäyttöalueiden poliittinen vakaus ja turvallisuustilanne, mukaan lukien seuraavat seikat:
 - i. voimassa olevat lait, mukaan lukien tietoturvaa koskevat lait
 - ii. voimassa olevat lainvalvontasäännökset
 - iii. maksukyvyttömyyslain säännökset, joita sovellettaisiin, jos palveluntarjoaja joutuisi vararikkoon, ja tästä seuraavat mahdolliset rajoitteet, erityisesti laitoksen ja maksulaitoksen tietojen kiireellisen palauttamisen osalta
- e. määrittää ja päättää tietojen luottamuksellisuuden asianmukainen suojataso, ulkoistettavien toimien jatkuvuus ja tietojen sekä järjestelmien eheys ja jäljitettävyys suunnitellun ulkoistamisen puitteissa. Laitosten ja maksulaitosten tulee myös harkita tarvittaessa erityistoimenpiteitä siirrettävälle tiedolle, muistissa olevalle tiedolle ja kyseisellä hetkellä käyttämättömille tiedoille, kuten salaustekniikat sekä asianmukainen avaintenhallinta-arkkitehtuuri
- f. tarkastella, onko palveluntarjoaja laitoksen tytäryhtiö tai emoyhtiö, kuuluuko se tilinpäätösten konsolidointiin tai laitosten suojajärjestelmään tai omistavatko sen laitosten suojajärjestelmään kuuluvat laitokset, ja arvioida tässä tapauksessa, miten suuri määräysvalta laitoksella on ja missä määrin se pystyy vaikuttamaan palveluntarjoajan toimintaan 2 jakson mukaisesti.

12.3 Due diligence

69. Ennen ulkoistamisjärjestelyn toteuttamista ja ulkoistettavaan toimintoon liittyvien operatiivisten riskien huomioimista laitosten ja maksulaitosten tulee varmistaa valitun palveluntarjoajan soveltuvuus arviointiprosessin avulla.
70. Jos kyseessä ovat kriittiset tai tärkeät toiminnot, laitosten ja maksulaitosten tulee varmistaa, että palveluntarjoajalla on tarvittava maine sekä soveltuva ja riittävä pätevyys, asiantuntemus, valmiudet, resurssit (esim. henkilö-, IT- ja rahoitusresurssit), organisaatorakenne sekä tarvittaessa toimilupa/toimiluvat tai rekisteröinti, jotka vaaditaan kriittisen tai tärkeän toiminnon luotettavaan ja ammattitaitoiseen tarjoamiseen sekä veloitteiden täyttämiseen sopimusluonnoksen voimassaolon aikana.
71. Palveluntarjoajan due diligence -tarkastuksessa tulee huomioida esimerkiksi seuraavat seikat:
- a. liiketoimintamalli, liiketoiminnan luonne, laajuus ja monimutkaisuus, taloudellinen tilanne, omistus ja ryhmän rakenne
 - b. pitkäaikaiset suhteet sellaisiin palveluntarjoajiin, jotka on jo arvioitu ja jotka tarjoavat palveluita laitokselle tai maksulaitokselle
 - c. onko palveluntarjoaja laitoksen tai maksulaitoksen emoyhtiö tai tytäryhtiö, kuuluuko se laitoksen konsolidoinnin piiriin tai kuuluuko se samaan laitosten suojajärjestelmään kuin laitos tai omistavatko sen samaan laitosten suojajärjestelmään kuuluvat laitokset
 - d. valvovatko toimivaltaiset viranomaiset palveluntarjoajan toimintaa.
72. Kun ulkoistamiseen liittyy henkilötietojen tai luottamuksellisten tietojen käsittely, laitosten ja maksulaitosten tulee varmistaa, että palveluntarjoaja suojaa tiedot asianmukaisilla teknisillä ja organisatorisilla toimilla.
73. Laitosten ja maksulaitosten tulee varmistaa asianmukaisilla toimilla, että palveluntarjoajat toimivat arvojensa ja menettelytapahjeidensa mukaisesti. Jos palveluntarjoajat ja niiden mahdolliset alihankkijat ovat sijoittautuneet kolmansiin maihin, laitosten ja maksulaitosten tulee erityisestivarmistaa, että palveluntarjoajan toiminta on eettistä ja sosiaalisesti vastuullista ja että palveluntarjoaja noudattaa kansainvälisiä ihmisoikeusnormeja (kuten Euroopan ihmisoikeussopimusta) sekä ympäristönsuojelua ja asianmukaisia työolosuhteita koskevia normeja, mukaan lukien lapsityövoiman kieltäminen.

13 Sopimuksetekovaihe

74. Laitoksen, maksulaitoksen ja palveluntarjoajan oikeudet ja velvollisuudet tulee määrittää selkeästi ja esittää kirjallisessa sopimuksessa.
75. Kriittisiä tai tärkeitä toimintoja koskevassa ulkoistamissopimuksessa tulee olla vähintään seuraavat tiedot:
- a. ulkoistettavan toiminnon selkeä kuvaus
 - b. sopimuksen alkamispäivä ja tarvittaessa päättymispäivä sekä palveluntarjoajaa ja laitosta tai maksulaitosta koskevat irtisanomisajat
 - c. sopimukseen sovellettava laki
 - d. osapuolten taloudelliset velvoitteet
 - e. tieto siitä, onko kriittisten tai tärkeiden toimintojen tai niiden oleellisten osien ulkoistaminen edelleen sallittua, ja jos on, 13.1 jaksossa määritetyt edelleen ulkoistamista koskevat ehdot
 - f. sijainti tai sijainnit (alueet tai maat), joissa kriittistä tai tärkeää toimintoa tarjotaan ja/tai joissa oleelliset tiedot sijaitsevat ja joissa niitä käsitellään, mahdollinen säilytyspaikka mukaan lukien, sekä noudatettavat ehdot, mukaan lukien velvollisuus ilmoittaa laitokselle tai maksulaitokselle, jos palveluntarjoaja ehdottaa kyseisten sijaintien muuttamista
 - g. tarvittaessa oleellisten tietojen saatavuuteen, käytettävyyteen, eheyteen, luottamuksellisuuteen ja turvallisuuteen liittyvät säännökset 13.2 jakson mukaisesti
 - h. laitoksen tai maksulaitoksen oikeus valvoa palveluntarjoajan toimintaa jatkuvasti
 - i. sovitut palvelutasot, mukaan lukien ulkoistetun toiminnon täsmälliset määrälliset ja laadulliset suoritustavoitteet oikea-aikaista seuranta varten, jotta korjaaviin toimenpiteisiin voidaan ryhtyä viipymättä, jos sovittua palvelutasoa ei saavuteta
 - j. palveluntarjoajan raportointivelvollisuudet laitokselle tai maksulaitokselle, mukaan lukien palveluntarjoajan ilmoitukset mahdollisista seikoista, jotka voivat vaikuttaa oleellisesti palveluntarjoajan kykyyn suorittaa kriittinen tai tärkeä toiminto tehokkaasti sovitun palvelutason mukaisesti sekä noudattaa sovellettavia lakeja ja sääntelyvaatimuksia, sekä tarvittaessa velvollisuus toimittaa raportteja palveluntarjoajan sisäiselle tarkastustoiminnolle
 - k. tieto siitä, onko palveluntarjoajan otettava pakollinen vakuutus tiettyjä riskejä vastaan ja vaadittu vakuutusturva tarvittaessa

- l. liiketoiminnan jatkuvuussuunnitelmien toteuttamista ja testaamista koskevat vaatimukset
- m. säännökset, joilla varmistetaan pääsy laitoksen tai maksulaitoksen omistamiin tietoihin siinä tapauksessa, että palveluntarjoaja on maksukyvytön tai kriisinratkaisun kohteena tai lopettaa liiketoiminnan
- n. palveluntarjoajan velvollisuus tehdä yhteistyötä laitoksen tai maksulaitoksen toimivaltaisten viranomaisten ja kriisinratkaisuviranomaisten kanssa sekä niiden nimittämien muiden henkilöiden kanssa
- o. jos kyseessä on laitos, sopimuksessa tulee viitata selkeästi kansallisen kriisinratkaisuviranomaiseen toimivaltaan ja erityisesti direktiivin 2014/59/EU (pankkien elvytys- ja kriisinratkaisudirektiivi) 68 ja 71 artiklaan ja kuvata erityisesti aineelliset sopimusvelvoitteet saman direktiivin 68 artiklan tarkoittamassa merkityksessä
- p. laitosten, maksulaitosten ja toimivaltaisten viranomaisten rajoittamattomat tarkastusoikeudet ulkoistettuihin palveluihin ja erityisesti kriittisiin tai tärkeisiin ulkoistettuihin palveluihin 13.3 jakson mukaisesti
- q. purkuoikeus 13.4 jakson mukaisesti.

13.1 Kriittisten tai tärkeiden toimintojen ulkoistaminen edelleen

- 76. Ulkoistamissopimuksessatulee määrittää, onko kriittisten tai tärkeiden toimintojen tai niiden oleellisten osien ulkoistaminen edelleen sallittua.
- 77. Jos kriittisten tai tärkeiden toimintojen ulkoistaminen edelleen on sallittua, laitosten ja maksulaitosten tulee määrittää, onko toiminnon edelleen ulkoistettava osa itsessään kriittinen tai tärkeä (eli oleellinen osa kriittistä tai tärkeää toimintoa), ja kirjata se siinä tapauksessa rekisteriin.
- 78. Jos kriittisten tai tärkeiden toimintojen ulkoistaminen edelleen on sallittua, kirjallisessa sopimuksessa on:
 - a. määritettävä mahdolliset tehtävätyypit, joita ei voida ulkoistaa edelleen
 - b. määritettävä ehdot, joita tulee noudattaa edelleen ulkoistamisessa
 - c. täsmennettävä, että palveluntarjoaja on velvollinen valvomaan edelleen ulkoistamiaan palveluita ja varmistamaan, että palveluntarjoajan ja laitoksen tai maksulaitoksen välisiä sopimusvelvoitteita noudatetaan jatkuvasti

- d. vaadittava palveluntarjoajaa pyytämään laitokselta tai maksulaitokselta täsmällisen tai yleisen kirjallisen luvan ennen tietojen ulkoistamista edelleen³⁴
 - e. veloitettava palveluntarjoajaa ilmoittamaan laitokselle tai maksulaitokselle suunnitellusta edelleen ulkoistamisesta tai siihen liittyvistä oleellisista muutoksista erityisesti silloin, kun se voi vaikuttaa palveluntarjoajan kykyyn noudattaa ulkoistamissopimuksen mukaisia velvollisuuksia. Tämä koskee myös alihankkijoiden suunnittelemaa merkittäviä muutoksia ja ilmoitusaikaa. Ilmoitusaika tulee määrittää siten, että ulkoistavalla laitoksella tai maksulaitoksella on vähintään aikaa tehdä ehdotettujen muutosten riskinarviointi ja vastustaa muutoksia, ennen kuin suunniteltu edelleen ulkoistaminen tai sen oleelliset muutokset toteutetaan
 - f. varmistettava tarvittaessa, että laitoksella tai maksulaitoksella on oikeus vastustaa suunniteltua edelleen ulkoistamista tai sen oleellisia muutoksia tai että nimenomainen hyväksyntä tarvitaan
 - g. varmistettava, että laitoksella tai maksulaitoksella on sopimukseen perustuva oikeus päättää sopimus tarpeettoman edelleen ulkoistamisen vuoksi esimerkiksi silloin, kun edelleen ulkoistaminen lisää oleellisesti laitoksen tai maksulaitoksen riskejä tai kun palveluntarjoaja ulkoistaa palveluita edelleen ilmoittamatta siitä laitokselle tai maksulaitokselle.
79. Laitokset ja maksulaitokset voivat hyväksyä edelleen ulkoistamisen vain siinä tapauksessa, että alihankkija sitoutuu seuraaviin ehtoihin:
- a. noudattamaan kaikkia sovellettavia lakeja, sääntelyvaatimuksia ja sopimusvelvoitteita
 - b. myöntämään laitokselle, maksulaitokselle ja toimivaltaiselle viranomaiselle samat pääsyä ja tarkastusta koskevat sopimusvelvoitteet kuin palveluntarjoaja.
80. Laitosten ja maksulaitosten tulee varmistaa, että palveluntarjoaja valvoo edelleen ulkoistettujen palveluiden tarjoajia asianmukaisesti ja laitoksen tai maksulaitoksen määrittämän käytännön mukaisesti. Jos ehdotettu edelleen ulkoistaminen voi aiheuttaa oleellista haittaa kriittisen tai tärkeän toiminnon ulkoistamisjärjestelylle tai suurentaa riskiä oleellisesti, mukaan lukien tilanteet, joissa 79 kohdassa määritetyt ehdot eivät täyty, laitoksen tai maksulaitoksen tulee käyttää oikeuttaan vastustaa edelleen ulkoistamista, jos tällaisesta oikeudesta on sovittu, ja/tai päättää sopimus.

13.2 Tietojen ja järjestelmien turvallisuus

81. Laitosten ja maksulaitosten tulee varmistaa, että palveluntarjoajat noudattavat tarvittaessa asianmukaisia tietotekniikan turvallisuusstandardeja.

³⁴ Katso asetuksen (EU) 2016/679 28 artikla.

82. Laitosten ja maksulaitosten tulee tarvittaessa (esimerkiksi silloin, kun kyse on pilvipalveluiden tai muiden ICT-palveluiden ulkoistamisesta) määrittää tietoturva ja järjestelmien tietoturva koskevat vaatimukset ulkoistamissopimuksessa ja valvoa jatkuvasti näiden vaatimusten noudattamista.
83. Jos palveluita ulkoistetaan pilvipalveluiden tarjoajille tai ulkoistamissopimukseen sisältyy henkilötietojen tai luottamuksellisten tietojen käsittelyä tai siirtoa, laitosten ja maksulaitosten tulee soveltaa riskiperusteista lähestymistapaa tietojen säilyttämiseen ja niiden käsittelypaikkaan (esim. maa tai alue) sekä tietoturvallisuutta koskeviin seikkoihin.
84. Rajoittamatta asetuksen (EU) 2016/679 vaatimuksia laitosten ja maksulaitosten tulee huomioida tietosuojaa koskevien kansallisten säädösten väliset erot ulkoistaessaan toimintoja (erityisesti kolmansiin maihin). Laitosten ja maksulaitosten tulee varmistaa, että ulkoistamissopimus velvoittaa palveluntarjoajan suojamaan luottamuksellisia tietoja, henkilötietoja tai muuten arkaluonteisia tietoja sekä noudattamaan kaikkia tietosuojaan liittyviä lakisääteisiä vaatimuksia, jotka koskevat laitoksia tai maksulaitoksia (esim. henkilötietojen suoja ja pankkisalaisuus tai vastaavat lakisääteiset luottamuksellisuusveloitteet, jotka koskevat asiakkaiden tietoja).

13.3 Oikeus päästä tietoihin ja saada tietoja sekä tarkastusoikeus

85. Laitosten ja maksulaitosten tulee varmistaa kirjallisella ulkoistamisjärjestelyllä, että sisäinen tarkastustoiminto pystyy tarkastamaan ulkoistetun toiminnon käyttämällä riskiperusteista lähestymistapaa.
86. Huolimatta ulkoistetun toiminnon kriittisyydestä tai tärkeydestä laitosten ja palveluntarjoajien välisissä kirjallisissa ulkoistamisjärjestelyissä tulee viitata toimivaltaisten viranomaisten ja kriisintarkastusviranomaisten direktiivin 2014/59/EU 63 artiklan 1 kohdan a alakohdan ja direktiivin 2013/36/EU 65 artiklan 3 kohdan mukaisesti tiedonkeräys- ja tutkintavaltuuksiin, jotka koskevat jäsenvaltioon sijoittautuneita palveluntarjoajia, ja varmistaa nämä oikeudet myös kolmansiin maihin sijoittautuneiden palveluntarjoajien osalta.
87. Mitä tulee kriittisten tai tärkeiden toimintojen ulkoistamiseen, laitosten ja maksulaitosten tulee varmistaa kirjallisella ulkoistamisjärjestelyllä, että palveluntarjoaja myöntää niille ja niiden toimivaltaisille viranomaisille, kriisintarkastusviranomaiset mukaan lukien, sekä muille laitosten tai toimivaltaisten viranomaisten nimeämille henkilöille seuraavat oikeudet:
 - a. täysi pääsy oleellisiin liiketoimintatiloihin (esim. päätoimipaikkaan ja operaatiokeskuksiin), mukaan lukien kaikki oleelliset laitteet, järjestelmät, verkot ja tiedot, joita käytetään ulkoistetun toiminnon tarjoamiseen, sekä oleelliset taloudelliset tiedot, henkilöstö ja palveluntarjoajan ulkoiset tarkastajat (pääsy- ja tiedonsaantioikeudet)

- b. ulkoistamisjärjestelyyn liittyvät rajoittamattomat tarkastusoikeudet, jotta ne pystyvät valvomaan ulkoistamisjärjestelyä ja varmistamaan, että kaikkia sovellettavia sääntely- ja sopimusvelvoitteita noudatetaan.
88. Jos laitokset tai maksulaitokset ulkoistavat toimintoja, jotka eivät ole kriittisiä tai tärkeitä, niiden tulee varmistaa pääsy- ja tarkastusoikeudet 87 kohdan (a) ja (b) alakohdan sekä 13.3 jakson mukaisesti käyttämällä riskiperusteista mallia, jossa huomioidaan ulkoistetun toiminnon luonne ja siihen liittyvät operatiiviset ja maineriskit, skaalattavuus ja mahdolliset vaikutukset toimintojen jatkuvuuteen ja sopimuskauteen. Laitosten ja maksulaitosten tulee huomioida, että toiminnoista voi tulla ajan myötä kriittisiä tai tärkeitä.
89. Laitosten ja maksulaitosten tulee varmistaa, että ulkoistamisjärjestely tai muu sopimusjärjestely ei estä tai rajoita laitoksia, toimivaltaisia viranomaisia tai nimitettyjä kolmansia osapuolia harjoittamasta pääsy- ja tarkastusoikeuttaan tehokkaasti,
90. Laitosten ja maksulaitosten tulee harjoittaa pääsy- ja tarkastusoikeuttaan, määrittää tarkastusväli ja tarkastettavat alueet riskiperusteisella menetelmällä ja noudattaa oleellisia, yhteisesti hyväksytyjä kansallisia tai kansainvälisiä tarkastusstandardeja.³⁵
91. Rajoittamatta laitosten ja maksulaitosten lopullista vastuuta ulkoistamisjärjestelyistä, ne voivat hyödyntää seuraavia:
- a. saman palveluntarjoajan muiden asiakkaiden kanssa järjestettävät yhteiset tarkastukset, jotka ne ja kyseiset asiakkaat tai niiden nimittämä kolmas osapuoli tekevät, mikä tehostaa tarkastusressurssien käyttöä ja pienentää asiakkaiden ja palveluntarjoajan organisatorista taakkaa
 - b. palveluntarjoaja antaa saataville kolmannen osapuolen sertifiointit ja kolmannen osapuolen tai sisäiset tarkastuskertomukset.
92. Ulkoistaessaan kriittisiä tai tärkeitä toimintoja laitosten ja maksulaitosten tulee arvioida, ovatko 91 kohdan b alakohdassa tarkoitetut sertifiointit ja kertomukset riittäviä ja täyttävätkö ne lakisääteiset velvollisuudet, eivätkä ne saa ajan kuluessa luottaa yksinomaan näihin kertomuksiin.
93. Laitokset ja maksulaitokset voivat käyttää 91 kohdan (b) alakohdassa kuvattua menetelmää vain seuraavissa tapauksissa:
- a. ne ovat tyytyväisiä ulkoistetun toiminnon tarkastussuunnitelmaan
 - b. ne varmistavat, että sertifiointin tai tarkastuskertomuksen laajuus kattaa järjestelmät (eli prosessit, sovellukset, infrastruktuurin, tietokeskukset jne.) ja laitoksen tai

³⁵ Lisätietoa laitoksille on Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden 22 jaksossa: <https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889>

maksulaitoksen keskeiseksi määrittämät tarkastukset ja että oleellisia sääntelyvaatimuksia noudatetaan

- c. ne arvioivat säännöllisesti sertifiointien tai tarkastuskertomusten sisällön perusteellisesti ja varmistavat, että kertomukset ja sertifiointit eivät ole vanhentuneet
 - d. ne varmistavat, että sertifiointin tai tarkastuskertomusten tulevat versiot kattavat keskeiset järjestelmät ja tarkastukset
 - e. ne ovat tyytyväisiä sertifioidun tai tarkastuksia tekevän osapuolen soveltavuuteen (esim. sertifiointi- tai tarkastusyriyksen vuorottelun, pätevyyden, asiantuntemuksen ja tarkastettaviin tietoihin liittyvien todisteiden tutkimisen uudelleensuorittamisen tai niiden varmentamisen osalta)
 - f. ne luottavat siihen, että sertifiointit annetaan ja tarkastukset tehdään yleisesti tunnustettujen, oleellisten ammatillisten normien mukaisesti, ja niihin kuuluu käytössä olevien keskeisten kontrollien operatiivisen tehokkuuden testaaminen
 - g. niillä on sopimukseen perustuva oikeus pyytää laajentamaan sertifiointia tai tarkastuskertomusta koskemaan muita oleellisia järjestelmiä tai kontroleja edellyttäen, että soveltamisalan muutosta koskevien pyyntöjen määrä ja toistuvuus on kohtuullinen ja perusteltu riskinarvioinnin näkökulmasta
 - h. niillä säilyy sopimukseen perustuva oikeus tehdä halutessaan yksittäisiä tarkastuksia, jotka koskevat kriittisten tai tärkeiden toimintojen ulkoistamista.
94. Euroopan pankkiviranomaisen valvonta- ja arviointiprosessin (SREP) yhteydessä tehtävää ICT-riskien arviointia koskevien ohjeiden mukaisesti laitosten tulee tarvittaessavarmistaa, että ne pystyvät tekemään tietoturvallisuuden penetraatiotestauksen, jolla arvioidaan toteutettujen kybertoimenpiteiden ja yhtiön sisäisten ICT:n tietoturvatoimenpiteiden tehokkuus.³⁶ Maksulaitoksilla tulee olla I osaston mukaisesti sisäiset ICT-riskeihin liittyvät kontrollimekanismit, mukaan lukien ICT-turvallisuuteen liittyvät kontrollit ja riskien pienentämiseen tähtäävät toimet.
95. Laitosten, maksulaitosten, toimivaltaisten viranomaisten ja tarkastajien tai niiden puolesta toimivien kolmansien osapuolten tulee ilmoittaa suunnitellusta tarkastuskäynnistä palveluntarjoajalle hyvissä ajoin ennen käyntiä, paitsi siinä tapauksessa, että se ei ole mahdollista hätä- tai kriisitilanteessa tai johtaisi siihen, että tarkastus menettäisi tehonsa.
96. Kun tarkastuksia tehdään moniasiakasympäristössä, toisen asiakkaan ympäristöön kohdistuvat riskit (kuten vaikutukset palvelutasoon, tietojen saatavuuteen ja luottamuksellisuuteen) on vältettävä tai ehkäistävä.

³⁶ Katso myös Euroopan pankkiviranomaisen ICT-riskejä koskevat ohjeet: <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>

97. Kun ulkoistamisjärjestely on teknisesti erittäin monimutkainen, kuten esimerkiksi pilvipalveluihin ulkoistamisessa, laitoksen tai maksulaitoksen tulee varmistaa, että tarkastuksen tekijällä (sisäisillä tarkastajilla, tarkastajaryhmällä tai sen puolesta toimivilla ulkoisilla tarkastajilla) on asianmukaiset ja oleelliset taidot ja tiedot tehokkaita tarkastuksia ja/tai arviointeja varten. Sama koskee kaikkia laitoksen tai maksulaitoksen työntekijöitä, jotka arvioivat palveluntarjoajien kolmannen osapuolen sertifiointeja tai tarkastuksia.

13.4 Purkamisoikeudet

98. Ulkoistamisjärjestelyssä tulee nimenomaisesti sallia se mahdollisuus, että laitos tai maksulaitos purkaa järjestelyn sovellettavan lain mukaisesti. Tämä koskee esimerkiksi seuraavia tilanteita:

- a. ulkoistettujen palveluiden tarjoaja rikkoo lakia, säädöksiä tai sopimusehtoja
- b. tunnistetaan esteitä, jotka voivat heikentää ulkoistetun toiminnon suorittamista
- c. tapahtuu oleellisia muutoksia, jotka vaikuttavat ulkoistamisjärjestelyyn tai palveluntarjoajaan (esim. edelleen ulkoistaminen tai alihankkijoita koskevat muutokset)
- d. luottamuksellisten tietojen, henkilötietojen tai muuten arkaluonteisten tietojen hallintaan ja turvallisuuteen liittyy heikkouksia
- e. laitoksen tai maksulaitoksen toimivaltainen viranomainen ohjeistaa näin esimerkiksi siinä tapauksessa, että toimivaltainen viranomainen ei pysty ulkoistamisjärjestelyn vuoksi enää tehokkaasti valvomaan laitosta tai maksulaitosta.

99. Ulkoistamisjärjestelyn tulee helpottaa ulkoistetun toiminnon siirtoa toiselle palveluntarjoajalle tai palauttamista takaisin laitokselle tai maksulaitokselle. Tätä varten ulkoistamisjärjestelyssä on:

- a. määritettävä selkeästi nykyisen palveluntarjoajan velvollisuudet siinä tapauksessa, että ulkoistettu toiminto siirretään toiselle palveluntarjoajalle tai palautetaan takaisin laitokselle tai maksulaitokselle, tietojen käsittely mukaan lukien
- b. määritettävä asianmukainen siirtymäaika, jonka kuluessa palveluntarjoaja jatkaa ulkoistetun toiminnon tarjoamista ulkoistamisjärjestelyn päättymisen jälkeen, jotta keskeytysten riski pienenee
- c. veloitettava palveluntarjoajaa tukemaan laitosta tai maksulaitosta toiminnon järjestelmällisessä siirrosta, jos ulkoistamissopimus päättyy.

14 Ulkoistettujen toimintojen valvonta

100. Laitosten ja maksulaitosten tulee valvoa jatkuvasti palveluntarjoajien kaikkiin ulkoistamisjärjestelyihin liittyvää toimintaa soveltamalla riskeihin perustuvaa lähestymistapaa ja kiinnittää erityistä huomiota kriittisiin ja tärkeisiin palveluihin. Niiden tulee myösvalvoa, että tietojen saatavuus, eheys ja turvallisuus on varmistettu. Jos ulkoistetun toiminnon riski, luonne tai laajuus on muuttunut oleellisesti, laitosten ja maksulaitosten tulee arvioida toiminnon kriittisyys tai tärkeys uudelleen 4 jakson mukaisesti.
101. Laitosten ja maksulaitosten tulee soveltaa ulkoistamisjärjestelyiden valvontaan ja hallintaan asianmukaistaosaamista, huolellisuutta ja paneutumista .
102. Laitosten tulee päivittää riskinarvioinnit säännöllisesti 12.2 jakson mukaisesti ja raportoida ylimmälle hallintoelimelle säännöllisesti tunnistetuista riskeistä, jotka liittyvät kriittisten tai tärkeiden toimintojen ulkoistamiseen.
103. Laitosten ja maksulaitosten tulee valvoa ja hallita ulkoistamisjärjestelyistä johtuvia sisäisiä keskittämriskejä. Tässä tulee huomioida näiden ohjeiden 12.2 jakso.
104. Laitosten ja maksulaitosten tulee varmistaa jatkuvasti, että ulkoistamisjärjestelyt ja varsinkin kriittisiä tai tärkeitä toimintoja koskevat ulkoistamisjärjestelyt täyttävät asianmukaiset suorituskykyä ja laatua koskevat standardit niiden periaatteiden mukaisesti. Seuraavat seikat tulee varmistaa:
- a. laitokset saavat asianmukaiset raportit palveluntarjoajilta
 - b. ne arvioivat palveluntarjoajien toimintaa esimerkiksi keskeisillä suorituskykyindikaattoreilla, keskeisillä kontrolli-indikaattoreilla, palveluraporteilla, itse annetuilla todistuksilla ja riippumattomilla arvioinneilla
 - c. laitokset käyvät läpi kaikki palveluntarjoajan toimittamat muut oleelliset tiedot, kuten raportit liiketoiminnan jatkuvuuteen liittyvistä toimista ja testauksesta.
105. Laitosten tulee ryhtyä asianmukaisiin toimiin, jos ne huomaavat, että ulkoistetun toiminnon toteuttamisessa on puutteita. Laitosten ja maksulaitosten on seurattava erityisesti kaikkia merkkejä siitä, että palveluntarjoaja ei suorita ulkoistettua kriittistä tai tärkeää toimintoa tehokkaasti tai sovellettavien lakien ja sääntelyvaatimusten mukaisesti. Jos puutteita tunnistetaan, laitosten ja maksulaitosten tulee ryhtyä asianmukaisiin korjaaviin toimiin tai oikaisutoimiin. Näihin voi lukeutua ulkoistamissopimuksen välitön purkaminen, jos se on tarpeen.

15 Irtautumisstrategiat

106. Kun kriittisiä tai tärkeitä toimintoja ulkoistetaan, laitoksilla ja maksulaitoksilla tulee olla dokumentoitu irtautumisstrategia, joka vastaa niiden ulkoistamiskperiaatteita tai

liiketoiminnan jatkuvuutta koskevia suunnitelmia.³⁷ Siinä tulee huomioida vähintään seuraavat mahdollisuudet:

- a. ulkoistamisjärjestely päättyy
- b. palveluntarjoaja ei kykene tarjoamaan palvelua
- c. toteutetun toiminnon laatu heikkenee ja toiminnon epäasiallinen toteuttaminen tai toteuttamatta jättäminen aiheuttaa todellisia tai mahdollisia liiketoiminnan keskeytyksiä
- d. toiminnon asianmukaiseen ja jatkuvaan soveltamiseen liittyy olennaisia riskejä.

107. Laitosten ja maksulaitosten tulee varmistaa, että ne pystyvät irtautumaan ulkoistamisjärjestelyistä ilman aiheettomia liiketoiminnan keskeytyksiä ja ilman, että ne joutuvat rajoittamaan sääntelyvaatimusten noudattamista tai että siitä on haittaa asiakkaille tarjottavien palveluiden jatkuvuudelle ja laadulle. Tätä varten niiden on:

- a. kehitettävä ja toteutettava irtautumissuunnitelmat, jotka ovat kattavia, dokumentoituja ja tarvittaessa riittävällä tavalla testattuja (esim. analysoimalla mahdolliset kustannukset, vaikutukset, resurssit ja ajalliset seuraamukset, jotka koituvat ulkoistetun palvelun siirtämisestä vaihtoehtoiselle palveluntarjoajalle)
- b. tunnistettava vaihtoehtoiset ratkaisut ja laadittava siirtymäsuunnitelmat, jotta laitos tai maksulaitos pystyy poistamaan ulkoistetut toiminnot ja tiedot palveluntarjoajalta ja siirtämään ne vaihtoehtoisille palveluntarjoajille tai palauttamaan ne laitokselle tai maksulaitokselle tai ryhtymään muihin toimiin, joilla pystytään varmistamaan kriittisen tai tärkeän toiminnon tai liiketoiminnon toteuttaminen kontrolloidulla ja riittävästi testatulla tavalla, jossa huomioidaan tietojen sijainnin mahdollisesti aiheuttamat haasteet, sekä ryhtymään tarvittaviin toimiin, jotta liiketoiminnan jatkuvuus voidaan varmistaa siirtymävaiheen aikana.

108. Laatiessaan irtautumisstrategioita laitosten ja maksulaitosten tulee:

- a. määrittää irtautumisstrategian tavoitteet
- b. tehdä liiketoiminnan vaikutusanalyysi, joka on oikeassa suhteessa ulkoistettujen prosessien, palveluiden tai tehtävien aiheuttamaan riskiin ja jossa tunnistetaan, mitä inhimillisiä ja taloudellisia resursseja tarvitaan irtautumissuunnitelman toteuttamiseen ja miten paljon aikaa se vie

³⁷Direktiivin 2013/36/EU 85 artiklan 2 kohdan ja Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden VI osaston mukaisesti laitoksilla ja maksulaitoksilla on oltava käytössä ulkoistettujen kriittisten tai tärkeiden toimintojen asianmukaiset liiketoiminnan jatkuvuutta koskevat suunnitelmat.

- c. osoittaa tehtävät, vastuut ja riittävät resurssit irtautumissuunnitelmien hallintaa ja toimien siirtämistä varten
- d. määrittää ulkoistettujen toimintojen ja tietojen onnistuneen siirron kriteerit
- e. määrittää indikaattorit, joita käytetään ulkoistamisjärjestelyn seurannassa (kuten 14 jaksossa on kuvattu), mukaan lukien palvelutasot, joita ei voida pitää hyväksyttävänä ja jotka johtavat irtautumiseen.

V osasto – toimivaltaisille viranomaisille suunnatut ulkoistamista koskevat ohjeet

109. Kun toimivaltaiset viranomaiset laativat asianmukaisia menettelyjä, joilla valvotaan, noudattavatko laitokset ja maksulaitokset toimiluvan myöntämisen edellytyksiä, tulee pyrkiä tunnistamaan, muuttavatko ulkoistamisjärjestelyt oleellisesti laitosten ja maksulaitosten toimiluvan myöntämisen edellytyksiä ja velvollisuuksia.
110. Toimivaltaisten viranomaisten tulee varmistaa, että ne voivat tehokkaasti valvoa laitoksia ja maksulaitoksia ja sitä, että laitokset ja maksulaitokset ovat varmistaneet ulkoistamisjärjestelyissään, että palveluntarjoajilla on velvollisuus myöntää toimivaltaiselle viranomaiselle ja laitokselle tarkastus- ja pääsyoikeus 13.3 jakson mukaisesti.
111. Laitoksen ulkoistamisriskien analysointi tulee tehdä vähintään valvonta- ja arviointiprosessin (SREP) yhteydessä, tai jos kyseessä on maksulaitos, osana muita valvontaprosesseja, tapauskohtaiset pyynnöt mukaan lukien, tai tarkastuskäyntien yhteydessä.
112. 11 jaksossa tarkoitettujen rekisteriin tallennettujen tietojen lisäksi toimivaltaiset viranomaiset voivat pyytää laitoksilta ja maksulaitoksilta lisätietoja erityisesti kriittisistä ja tärkeistä ulkoistamisjärjestelyistä. Tällaisia ovat esimerkiksi:
- a. yksityiskohtainen riskianalyysi
 - b. tieto siitä, onko palveluntarjoajalla liiketoiminnan jatkuvuussuunnitelma, joka soveltuu ulkoistavalle laitokselle tai maksulaitokselle tarjottaviin palveluihin
 - c. irtautumisstrategia, jota sovelletaan jos jompikumpi osapuoli päättää ulkoistamisjärjestelyn tai jos palveluiden toimittamisessa on häiriöitä
 - d. käytössä olevat resurssit ja toimet, joilla voidaan valvoa ulkoistettuja tehtäviä riittävällä tavalla.
113. 11 jakson mukaisesti vaadittujen tietojen lisäksi toimivaltaiset viranomaiset voivat pyytää laitoksia tai maksulaitoksia toimittamaan yksityiskohtaisia tietoja mistä tahansa ulkoistamisjärjestelystä, vaikka kyseistä toimintoa ei pidettäisi kriittisenä tai tärkeänä.

114. Toimivaltaisten viranomaisten tulee arvioida seuraavat seikat noudattamalla riskiperusteista menetelmää:
- a. valvovatko ja hallitsevatko laitokset ja maksulaitokset ulkoistettuja järjestelyjä ja erityisesti ulkoistettuja kriittisiä tai tärkeitä toimintoja asianmukaisesti
 - b. onko laitoksilla ja maksulaitoksilla käytössä riittävästi resursseja ulkoistamisjärjestelyiden valvontaa ja hallintaa varten
 - c. tunnistavatko laitokset ja maksulaitokset kaikki oleelliset riskit ja pystyvätkö ne hallitsemaan niitä
 - d. tunnistavatko, arvioivatko ja hallitsevatko laitokset ja maksulaitokset asianmukaisesti ulkoistamisjärjestelyihin liittyviä eturistiriitoja esimerkiksi ryhmän sisäisissä ulkoistuksissa tai saman laitosten suojajärjestelmän sisällä tapahtuvissa ulkoistuksissa.
115. Toimivaltaisten viranomaisten tulee varmistaa, että EU:hun tai ETAan sijoittautuneet laitokset ja maksulaitokset eivät ole pelkkiä ”tyhjiä kuoria”. Tämä koskee myös tilanteita, joissa laitokset siirtävät osan markkina- ja luottoriskistä back-to-back-kaupoilla tai ryhmän sisäisillä kaupoilla laitokseen, joka on sijoittautunut EU:n tai ETAn ulkopuolelle. Toimivaltaisten viranomaisten tulee varmistaa, että laitoksilla on riskien tunnistamiseen ja hallintaan tarvittavat asianmukaiset hallinta- ja riskienhallintajärjestelyt.
116. Toimivaltaisten viranomaisten tulee huomioida arvioinnissa kaikki erityisesti seuraavat riskit:³⁸
- a. ulkoistamisjärjestelyistä johtuvat operatiiviset riskit³⁹
 - b. maineriskit
 - c. riski siitä, että laitos joutuu puuttumaan asioihin ja pelastamaan palveluntarjoajan, jos kyseessä on merkittävä laitos
 - d. laitoksen sisäiset keskittämiskit, myös konsolidoidulla tasolla, joita aiheuttavat useat ulkoistamisjärjestelyt samalle palveluntarjoajalle tai toisiinsa kytköksissä oleville palveluntarjoajille tai useat ulkoistamisjärjestelyt samalla liiketoiminnan osa-alueella
 - e. keskittämiskit sektorin tasolla esimerkiksi silloin, kun useat laitokset tai maksulaitokset käyttävät yhtä palveluntarjoajaa tai pientä palveluntarjoajien ryhmää

³⁸ Jos laitokseen sovelletaan direktiiviä 2013/36/EU, katso myös Euroopan pankkiviranomaisen valvonta- ja arviointiprosessia (SREP) koskevat ohjeet: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2>

³⁹ Katso myös Euroopan pankkiviranomaisen ICT-riskejä koskevat ohjeet: <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>

- f. ulkoistavan laitoksen tai maksulaitoksen määräysvalta palveluntarjoajaan tai mahdollisuus vaikuttaa sen toimintaan, ylemmän tason valvonnasta mahdollisesti johtuva riskien pieneneminen sekä se, kuuluuko palveluntarjoaja ryhmän konsolidoituun valvontaan
 - g. eturistiriidat laitoksen ja palveluntarjoajan välillä.
117. Jos keskittämriskejä havaitaan, toimivaltaisten viranomaisten tulee valvoa niiden kehittymistä ja arvioitava niiden mahdolliset vaikutukset muihin laitoksiin ja maksulaitoksiin sekä rahoitusmarkkinoiden vakauteen. Toimivaltaisten viranomaisten tulee tarvittaessa ilmoittaa kriisinratkaisuviranomaiselle uusista mahdollisesti kriittisistä toiminnoista⁴⁰, jotka on tunnistettu tämän arvioinnin aikana.
118. Jos havaitaan huolenaiheita, jotka johtavat siihen, että laitoksella tai maksulaitoksella ei enää ole luotettavia hallinnointi- ja ohjausjärjestelmiä tai se ei täytä sääntelyvaatimuksia, toimivaltaisten viranomaisten tulee ryhtyä asianmukaisiin toimiin, kuten rajoitettava ulkoistettujen toimintojen laajuutta tai veloitettava laitos irtautumaan yhdestä tai useasta ulkoistamisjärjestelystä. Laitoksen tai maksulaitoksen jatkuvan toimivuuden kannalta tulee erityisesti huomioida, että sopimusten peruuttaminen voi olla tarpeen, jos valvontaa ja sääntelyvaatimusten noudattamista ei voida varmistaa muilla keinoilla.
119. Toimivaltaisten viranomaisten tulee varmistaa, että ne pystyvät valvomaan laitoksia ja maksulaitoksia tehokkaasti erityisesti silloin, kun nämä ulkoistavat kriittisiä tai tärkeitä toimintoja, jotka toteutetaan EU:n tai ETAn ulkopuolella.

⁴⁰ Pankkien elvytys- ja kriisinratkaisudirektiivin 2 artiklan 1 kohdan 35 alakohdassa annetun määritelmän mukaisesti.