Ohjeet

EBA/GL/2019/04

28. marraskuuta 2019

Euroopan pankkiviranomaisen ohjeet tieto- ja viestintätekniikka- (ICT) sekä turvallisuusriskien hallinnasta

Noudattamista ja ilmoittamista koskevat velvoitteet

Näiden ohjeiden asema

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

2. Ohjeissa esitetään Euroopan pankkiviranomaisen (EPV) näkemys asianmukaisista Euroopan finanssivalvojien järjestelmässä toteutettavista valvontakäytännöistä ja siitä, miten unionin oikeutta olisi sovellettava tietyissä asioissa. Asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdassa määriteltyjen toimivaltaisten viranomaisten, joihin näitä ohjeita sovelletaan, on noudatettava ohjeita sisällyttämällä ne tarpeen mukaan valvontakäytäntöihinsä (esim. muuttamalla lainsäädäntöään tai valvontamenettelyjään). Tämä koskee myös ohjeita, jotka on suunnattu ensisijaisesti laitoksille.

Raportointivaatimukset

3. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan nojalla toimivaltaisten viranomaisten tulee ilmoittaa Euroopan pankkiviranomaiselle viimeistään pp.kk.vvvv, noudattavatko ne tai aikovatko ne noudattaa näitä ohjeita, sekä syyt niiden noudattamatta jättämiseen. Jos ilmoitusta ei toimiteta tähän määräaikaan mennessä, Euroopan pankkiviranomainen katsoo, etteivät toimivaltaiset viranomaiset noudata ohjeita. Ilmoitukset lähetetään Euroopan pankkiviranomaisen verkkosivustolla olevalla lomakkeella sähköpostitse osoitteeseen compliance@eba.europa.eu. Viitteeksi merkitään ”EBA/GL/2019/04”. Ilmoituksen voi lähettää ainoastaan henkilö, jolla on asianmukaiset valtuudet ilmoittaa ohjeiden noudattamisesta toimivaltaisen viranomaisen puolesta. Ohjeiden noudattamisen osalta tehtävistä muutoksista tulee myös 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).

Aihe, soveltamisala ja määritelmät

Kohde

5. Nämä ohjeet perustuvat direktiivin 2013/36/EU (vakavaraisuusdirektiivi) 74 artiklan sisäistä hallintaa koskeviin säännöksiin sekä toimeksiantoon antaa ohjeita direktiivin (EU) 2015/2366 (toinen maksupalveludirektiivi) 95 artiklan 3 kohdassa tarkoitetulla tavalla.

6. Näissä ohjeissa yksilöidään riskinhallintatoimenpiteet, joihin finanssilaitosten (jotka määritellään jäljempänä 5 kohdassa) on ryhdyttävä vakavaraisuusdirektiivin 74 artiklan mukaisesti tieto- ja viestintätekniikka- sekä turvallisuusriskiensä hallitsemiseksi kaikessa toiminnassa. Niissä myös täsmennetään, että maksupalveluntarjoajien (jotka määritetään jäljempänä 9 kohdassa) tulee varmistaa toisen maksupalveludirektiivin 95 artiklan 1 kohdan mukaisesti niiden tarjoamiin maksupalveluihin liittyvien operatiivisten ja turvallisuusriskien (joilla tarkoitetaan tieto- ja viestintätekniikka- sekä turvallisuusriskejä) hallinta. Ohjeisiin kuuluu tietoturvaa, myös kyberturvallisuutta, koskevia vaatimuksia siltä osin kuin tiedot ovat tieto- ja viestintäteknisissä järjestelmissä.

Soveltamisala

7. Näitä ohjeita sovelletaan tieto- ja viestintätekniikka (ICT)- sekä turvallisuusriskien hallintaan finanssilaitoksissa (jotka määritetään 9 kohdassa). Ohjeissa ICT- ja turvallisuusriskeillä tarkoitetaan toisen maksupalveludirektiivin 95 artiklan operatiivisia ja turvallisuusriskejä maksupalvelujen tarjonnassa.

8. Maksupalveluntarjoajien (jotka määritetään 9 kohdassa) osalta ohjeita sovelletaan niiden maksupalvelujen tarjoamiseen toisen maksupalveludirektiivin 95 artiklan soveltamisalan ja toimeksiannon mukaisesti. Laitosten (jotka määritetään 9 kohdassa) osalta ohjeita sovelletaan kaikkiin niiden tarjoamiin toimintoihin.

Osoitus

9. Nämä ohjeet on osoitettu finanssilaitoksille, joilla näissä ohjeissa tarkoitetaan 1) toisen maksupalveludirektiivin 4 artiklan 11 kohdassa määriteltyjä maksupalveluntarjoajia ja 2) laitoksia eli asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdan 3 alakohdassa määriteltyjä luottolaitoksia ja sijoituspalveluyrityksiä. Ohjeet koskevat myös asetuksen (EU) N:o 575/2013 4 artiklan 1 kohdan 40 alakohdassa määriteltyjä toimivaltaisia viranomaisia, muun muassa Euroopan keskuspankkia sille asetuksella (EU) N:o 1024/2013 annettuja tehtäviä koskevilta osin, sekä asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdan i alakohdassa tarkoitettuja toisen maksupalveludirektiivin soveltamisalaan kuuluvia toimivaltaisia viranomaisia.

Määritelmät

10. Ellei toisin ole määritetty, vakavaraisuusdirektiivissä 2013/36/EU, vakavaraisuusasetuksessa (EU) N:o 575/2013 ja toisessa maksupalveludirektiivissä (EU) 2015/2366 käytettyjen ja määriteltyjen termien merkitykset ovat näissä ohjeissa samat. Lisäksi näissä ohjeissa käytetään seuraavia määritelmiä:

Tieto- ja viestintätekniikka- (ICT) sekä turvallisuusriski	Tappion riski, joka johtuu salassapitovelvollisuuden rikkomisesta, järjestelmien ja datan eheyden rikkoutumisesta, järjestelmien ja datan sopivuudessa tai saatavuudessa olevista ongelmista tai siitä, että tietotekniikkaa ei pystytä vaihtamaan kohtuullisen ajan kuluessa ja kohtuullisin kustannuksin, kun ympäristö- ja liiketoimintavaatimukset muuttuvat (ts. joustavuus) [2]. Tähän kuuluvat turvallisuusriskit, jotka johtuvat riittämättömistä tai epäonnistuneista sisäisistä prosesseista tai ulkoisista tapahtumista, muun muassa kyberhyökkäyksistä tai riittämättömästä fyysisestä turvallisuudesta.
Ylin hallintoelin	(a) Luottolaitosten ja sijoituspalveluyritysten osalta tällä termillä tarkoitetaan samaa kuin direktiivin 2013/36/EU 3 artiklan 1 kohdan 7 alakohdan määritelmällä. (b) Maksulaitosten tai sähköisen rahan liikkeeseenlaskijalaitosten osalta tällä termillä tarkoitetaan johtajia tai maksulaitosten tai sähköisen rahan liikkeeseenlaskijalaitosten johtotehtävistä vastuussa olevia henkilöitä ja, kun se on asianmukaista, maksulaitosten tai sähköisen rahan liikkeeseenlaskijalaitosten maksupalvelutoiminnan johtamisesta vastuussa olevia henkilöitä. (c) Direktiivin (EU) 2015/2366 1 artiklan 1 kohdan c, e ja f alakohdassa tarkoitettujen maksupalveluntarjoajien osalta tällä termillä tarkoitetaan samaa kuin sovellettavassa EU:n tai kansallisessa lainsäädännössä annetulla määritelmällä.
Operatiivinen poikkeama tai turvapoikkeama	Yksittäinen tapahtuma tai toisiinsa liittyvien tapahtumien sarja, jota finanssilaitos ei ole suunnitellut ja joka vaikuttaa tai todennäköisesti vaikuttaa haitallisesti palvelujen luotettavuuteen, saatavuuteen, luottamuksellisuuteen ja/tai aitouteen.
Toimiva johto	(a) Luottolaitosten ja sijoituspalveluyritysten osalta tällä termillä tarkoitetaan samaa kuin direktiivin 2013/36/EU 3 artiklan 1 kohdan 9 alakohdan määritelmällä.

[2] Määritelmä 19. joulukuuta 2014 annetuista Euroopan pankkiviranomaisen ohjeista valvojan arviointiprosessin (SREP) yhteisistä menettelyistä ja menetelmistä (EBA/GL/2014/13) sellaisina kuin ne ovat muutettuina tarkistetuilla ohjeilla EBA/GL/2018/03.

	(b) Maksulaitosten ja sähköisen rahan liikkeeseenlaskijalaitosten osalta tällä termillä tarkoitetaan luonnollisia henkilöitä, jotka vastaavat laitoksen päivittäisestä johtamisesta ja ovat siitä vastuussa ja tilivelvollisia ylimmälle hallintoelimelle. (c) Direktiivin (EU) 2015/2366 1 artiklan 1 kohdan c, e ja f alakohdassa tarkoitettujen maksupalveluntarjoajien osalta tällä termillä tarkoitetaan samaa kuin sovellettavassa EU:n tai kansallisessa lainsäädännössä annetulla määritelmällä.
Riskinottohalu	Niiden riskien yhteenlaskettu taso ja tyyppi, jotka maksupalveluntarjoajat ja laitokset ovat valmiita ottamaan riskinkantokykynsä rajoissa ja liiketoimintamallinsa mukaisesti saavuttaakseen strategiset tavoitteensa.
Tarkastustoiminto	(a) Luottolaitosten ja sijoituspalveluyritysten osalta tarkastustoiminnolla tarkoitetaan samaa kuin Euroopan pankkiviranomaisen hallintoa ja ohjausta koskevien ohjeiden (EBA/GL/2017/11) 22 kohdassa. (b) Muiden maksupalveluntarjoajien kuin luottolaitosten osalta tarkastustoiminnon tulee olla riippumaton maksupalveluntarjoajassa ja maksupalveluntarjoajasta, ja se voi olla sisäisen ja/tai ulkoisen tarkastuksen toiminto.
Tieto- ja viestintätekniikan hankkeet / ICT-hankkeet	Kaikki hankkeet tai niiden osat, joissa tieto- ja viestintäteknisiä järjestelmiä muutetaan, vaihdetaan, poistetaan tai toteutetaan. Tieto- ja viestintätekniikan hankkeet voivat olla osa laajempia tieto- ja viestintätekniikan tai liiketoiminnan muutosohjelmia.
Kolmas osapuoli	Organisaatio, joka on aloittanut liikesuhteen tai tehnyt sopimuksen yhteisön kanssa tarjotakseen tuotetta tai palvelua[3].
Tietoresurssit	Kokoelma aineellisia tai aineettomia tietoja, jotka ovat suojaamisen arvoisia.
Tieto- ja viestintätekniset resurssit / ICT-resurssit	Joko ohjelmisto- tai laitteistoresurssit, joita käytetään liiketoimintaympäristössä
Tieto- ja viestintätekniset järjestelmät[4] / ICT-järjestelmät	Tietyn mekanismin tai yhteiskäyttöverkon osana oleva tieto- ja viestintätekninen rakenne, jolla tuetaan laitoksen toimintoja.
Tieto- ja viestintätekniset palvelut[5] / ICT-palvelut	Palvelut, joita tieto- ja viestintätekniset järjestelmät tarjoavat yhdelle tai useammalle laitoksen sisäiselle tai ulkopuoliselle käyttäjälle. Tällaisia palveluja ovat esimerkiksi tiedon syöttö, tallennus ja käsittely sekä raportointipalvelut mutta myös seuranta sekä liiketoiminnan ja päätöksenteon tukipalvelut.

[3] Määritelmä G7-ryhmän perustekijöistä, jotka koskevat kolmannen osapuolen kyberriskin hallintaa rahoitusalalla.
[4] Määritelmä vakavaraisuuden arviointiprosessin (SREP) mukaisesta tieto- ja viestintätekniikkariskien arvioinnista annetuista tiedoista (EBA/GL/ 2017/05).
[5] Sama kuin edellä.

Täytäntöönpano

Soveltamispäivä

11. Nämä ohjeet tulevat voimaan 30. kesäkuuta 2020.

Kumoaminen

12. Näillä ohjeilla kumotaan vuonna 2017 annetut ohjeet maksupalvelujen operatiivisia riskejä ja turvallisuusriskejä koskevista turvatoimenpiteistä (EBA/GL/2017/17) näiden ohjeiden soveltamisen alkamispäivästä alkaen.

Ohjeet ICT- ja turvallisuusriskien hallinnasta

1.1. Suhteellisuus

1. Kaikkien finanssilaitosten on noudatettava näissä ohjeissa esitettyjä säännöksiä siten, että se on oikeassa suhteessa kunkin finanssilaitoksen kokoon, niiden sisäiseen organisaatioon ja sellaisten palvelujen ja tuotteiden luonteeseen, soveltamisalaan, monimutkaisuuteen ja riskialttiuteen nähden, joita finanssilaitokset tarjoavat tai aikovat tarjota, ja että siinä otetaan edellä mainitut tekijät huomioon.

1.2. Hallinto ja strategia

1.2.1. Hallinto

2. Ylimmän hallintoelimen tulee varmistaa, että finanssilaitoksilla on käytössä asianmukainen sisäisen hallinnon ja sisäisen valvonnan kehys niiden ICT- ja turvallisuusriskejä varten. Hallintoelimen tulee määrittää selkeät tehtävät ja vastuut tieto- ja viestintätekniikan toiminnoille, tietoturvan riskinhallinnalle ja liiketoiminnan jatkuvuudelle, myös ylimmän hallintoelimen ja sen komiteoiden osalta.
3. Ylimmän hallintoelimen tulee varmistaa, että finanssilaitosten henkilöstön määrä ja osaaminen ovat asianmukaisia niiden tieto- ja viestintätekniikan operatiivisten tarpeiden ja niiden ICT- ja turvallisuusriskien hallintaprosessien tukemiseksi jatkuvasti sekä niiden ICT-strategian toteuttamiseksi. Ylimmän hallintoelimen tulee varmistaa, että edellä mainitun toteuttamiseen on osoitettu riittävästi määrärahoja. Finanssilaitosten tulee lisäksi varmistaa, että kaikki työntekijät, myös keskeisistä toiminnoista vastaavat henkilöt, saavat asianmukaisen koulutuksen ICT- ja turvallisuusriskeistä, muun muassa tietoturvasta, vuosittain tai tarvittaessa useammin (ks. myös 1.4.7 jakso).

4. Ylimmällä hallintoelimellä on yleinen vastuuvelvollisuus finanssilaitosten ICT-strategian laatimisesta, hyväksymisestä ja toteuttamisen valvomisesta osana niiden yleistä liiketoimintastrategiaa sekä tehokkaan riskinhallintakehyksen luomisesta ICT- ja turvallisuusriskejä varten.

1.2.2. Strategia

5. ICT-strategiaa tulee yhdenmukaistaa finanssilaitosten yleisen liiketoimintastrategian kanssa, ja siinä tulee määrittää seuraavat:

    a) se, miten finanssilaitosten tieto- ja viestintätekniikkaa pitäisi kehittää, jotta sillä voitaisiin tukea tehokkaasti niiden liiketoimintastrategiaa ja osallistua siihen, muun muassa kehittämällä organisaatiorakennetta, ICT-järjestelmän muutoksia ja keskeisiä riippuvuuksia kolmansien osapuolten kanssa
    b) suunniteltu strategia ja ICT-arkkitehtuurin kehitys, myös kolmansia osapuolia koskevat riippuvuudet
    c) selkeät tietoturvatavoitteet, joissa keskitytään tieto- ja viestintäteknisiin järjestelmiin ja palveluihin, henkilöstöön ja prosesseihin.

6. Finanssilaitosten tulee laatia toimintasuunnitelmia, jotka sisältävät toimenpiteitä, joihin on ryhdyttävä ICT-strategian tavoitteen saavuttamiseksi. Niistä tulee tiedottaa kaikelle asianomaiselle henkilöstölle (myös alihankkijoille ja ulkopuolisille palveluntarjoajille, kun se on tarpeen ja merkityksellistä). Toimintasuunnitelmia tulee tarkistaa säännöllisesti niiden merkityksellisyyden ja asianmukaisuuden varmistamiseksi. Finanssilaitosten on myös laadittava prosessit ICT-strategiansa toteuttamisen tehokkuuden seuraamiseksi ja mittaamiseksi.

1.2.3. Ulkopuolisten palveluntarjoajien käyttö

7. Sanotun rajoittamatta Euroopan pankkiviranomaisen ulkoistamisesta antamia ohjeita (EBA/GL/2019/02) ja toisen maksupalveludirektiivin 19 artiklaa finanssilaitosten tulee varmistaa niiden riskinhallintakehyksessä määritettyjen riskinvähentämiskeinojen, myös näissä ohjeissa esitettyjen toimenpiteiden, tehokkuus, kun maksupalvelujen ja/tai ICT- palvelujen ja minkä tahansa toiminnon ICT-järjestelmien operatiivisia toimintoja ulkoistetaan, myös konsernin yhteisöille, tai kun käytetään kolmansia osapuolia.

8. ICT-palvelujen ja -järjestelmien jatkuvuuden varmistamiseksi finanssilaitosten tulee varmistaa, että sopimukset ja palvelutasosopimukset (sekä tavanomaisissa olosuhteissa että palvelun keskeytyessä – ks. myös 1.7.2 jakso) palveluntarjoajien (ulkoistamisen tarjoajat, konsernin yhteisöt tai ulkopuoliset palveluntarjoajat) kanssa sisältävät seuraavat:

    a) asianmukaiset ja oikeasuhteiset tietoturvaan liittyvät tavoitteet ja toimenpiteet, myös vaatimukset, kuten kyberturvallisuuden vähimmäisvaatimukset; finanssilaitosten tietojen elinkaaren eritelmät; kaikki tietojen salaamista koskevat vaatimukset, tietoverkon turvallisuus ja turvallisuuden valvontaprosessit ja konesalien sijainti
    b) operatiivisten poikkeamien ja turvallisuuspoikkeamien käsittelymenettelyt, myös eskaloinnin ja raportoinnin osalta.

9. Finanssilaitosten tulee valvoa sitä, millä tasolla nämä finanssilaitokset noudattavat turvallisuustavoitteita, turvatoimenpiteitä ja suoritustavoitteita, ja pyrittävä saamaan varmistus siitä.

1.3. ICT- ja turvallisuusriskien hallintakehys

1.3.1. Järjestäminen ja tavoitteet

10. Finanssilaitosten tulee tunnistaa ICT- ja turvallisuusriskinsä ja hallittava niitä. ICT-järjestelmistä, prosesseista ja turvallisuusoperaatioista vastaavilla ICT-toiminnoilla tulee olla käytössä asianmukaiset prosessit ja kontrollit sen varmistamiseksi, että kaikki riskit havaitaan, analysoidaan ja mitataan, niitä seurataan ja hallitaan, niistä raportoidaan ja ne pidetään finanssilaitoksen riskinottohalun rajoissa ja että niiden toteuttamissa projekteissa ja järjestelmissä sekä niiden suorittamissa toiminnoissa noudatetaan ulkoisia ja sisäisiä vaatimuksia.

11. Finanssilaitosten tulee osoittaa vastuu ICT- ja turvallisuusriskien hallinnasta ja seurannasta valvontatoiminnolle hallinnosta ja ohjauksesta annettujen Euroopan pankkiviranomaisen ohjeiden (EBA/GL/2017/11) 19 kohdan vaatimusten mukaisesti. Finanssilaitosten tulee varmistaa tämän valvontatoiminnon riippumattomuus ja puolueettomuus erottamalla ICT-operaatioiden prosessit siitä asianmukaisesti. Tämän valvontatoiminnon tulee olla suoraan vastuussa ylimmälle hallintoelimelle, ja sen tulee vastata ICT- ja turvallisuusriskien hallintakehyksen noudattamisen seurannasta ja valvonnasta. Sen tulee varmistaa, että ICT- ja turvallisuusriskit havaitaan, mitataan ja arvioidaan, niitä hallitaan ja valvotaan ja niistä raportoidaan. Finanssilaitosten tulee varmistaa, että tämä valvontatoiminto ei ole vastuussa sisäisistä tarkastuksista.

    Sisäisen tarkastuksen toiminnolla tulee riskipohjaisen lähestymistavan perusteella olla valmiudet tarkastaa itsenäisesti, että kaikissa finanssilaitoksen tieto- ja viestintätekniikkaan ja turvallisuuteen liittyvissä toiminnoissa ja yksiköissä noudatetaan finanssilaitoksen toimintamalleja ja menettelyjä sekä ulkoisia vaatimuksia, ja valmiudet antaa siitä puolueeton varmistus hallinnosta ja ohjauksesta annettujen Euroopan pankkiviranomaisen ohjeiden (EBA/GL/2017/11) 22 kohdan vaatimuksia noudattaen.

12. Finanssilaitosten tulee määrittää ja osoittaa keskeiset tehtävät ja vastuut ja asiaankuuluvat raportointisuhteet, jotta ICT- ja turvallisuusriskien hallintakehys olisi tehokas. Tämä kehys tulee yhdistää täysimääräisesti finanssilaitosten yleisiin riskienhallintaprosesseihin ja yhdenmukaistaa niiden kanssa.

13. ICT- ja turvallisuusriskien hallintakehyksessä tulee olla käytössä prosesseja, joilla

    a) määritetään ICT- ja turvallisuusriskejä koskeva riskinottohalu finanssilaitoksen riskinottohalun mukaisesti
    b) tunnistetaan ja arvioidaan ICT- ja turvallisuusriskit, joille finanssilaitos on altis
    c) määritetään vähentämiskeinot, myös kontrollit, joilla ICT- ja turvallisuusriskejä voidaan vähentää

d) seurataan näiden toimenpiteiden tehokkuutta sekä raportoitujen poikkeamien määrää, myös maksupalveluntarjoajien osalta toisen maksupalveludirektiivin 96 artiklan mukaisesti raportoituja poikkeamia, jotka vaikuttavat tieto- ja viestintätekniikkaan liittyviin toimintoihin, ja ryhdytään tarvittaessa toimiin toimenpiteiden korjaamiseksi
e) raportoidaan ylimmälle hallintoelimelle ICT- ja turvallisuusriskeistä ja niiden kontrolleista
f) tunnistetaan ja arvioidaan, johtuvatko ICT- ja turvallisuusriskit merkittävästä muutoksesta ICT- järjestelmissä tai ICT-palveluissa, -prosesseissa tai -menettelyissä ja/tai merkittävästä operatiivisesta poikkeamasta tai turvapoikkeamasta.

14. Finanssilaitosten tulee varmistaa, että ICT- ja turvallisuusriskien hallintakehys dokumentoidaan ja että sitä parannetaan jatkuvasti sen toteuttamisen ja valvonnan aikana saatujen kokemusten perusteella. Ylimmän hallintoelimen tulee hyväksyä ICT- ja turvallisuusriskien hallintakehys ja tarkistaa se vähintään kerran vuodessa.

1.3.2. Toimintojen, prosessien ja resurssien tunnistaminen

15. Finanssilaitosten tulee tunnistaa liiketoimintonsa, tehtävänsä ja tukiprosessinsa, vahvistaa ne ja ylläpitää niistä ajan tasalla olevaa kartoitusta, jotta voitaisiin tunnistaa niiden kunkin merkitys ja niiden keskinäiset riippuvuudet ICT- ja turvallisuusriskien osalta.

16. Finanssilaitosten tulee lisäksi tunnistaa liiketoimintojaan ja tukiprosessejaan tukevat tietoresurssit, vahvistaa ne ja ylläpitää niistä ajan tasalla olevaa kartoitusta, jotta voitaisiin vähintäänkin hallita tietoresursseja, jotka tukevat niiden kriittisiä liiketoiminnan toimintoja ja prosesseja, ja ottaa huomioon niiden riippuvuudet muista sisäisistä ja ulkoisista järjestelmistä ja prosesseista. Resursseja ovat muun muassa ICT-järjestelmät, henkilöstö, palveluntarjoajat ja kolmannet osapuolet.

1.3.3. Luokitus ja riskiarviointi

17. Finanssilaitosten tulee luokitella 15 ja 16 kohdassa tarkoitetut tunnistetut liiketoiminnot, tukiprosessit ja tietoresurssit niiden kriittisyyden perusteella.

18. Näiden tunnistettujen liiketoimintojen, tukiprosessien ja tietoresurssien kriittisyyden määrittämiseksi finanssilaitosten tulee vähintään ottaa huomioon luottamuksellisuutta, eheyttä ja saatavuutta koskevat vaatimukset. Tietoresurssien osalta tulee osoittaa selkeästi vastuuvelvollisuus ja vastuu.

19. Finanssilaitosten tulee tarkastaa tietoresurssien luokituksen asianmukaisuus ja asiaankuuluvat asiakirjat, kun riskinarviointi tehdään.

20. Finanssilaitosten tulee tunnistaa ICT- ja turvallisuusriskit, jotka vaikuttavat tunnistettuihin ja luokiteltuihin liiketoimintoihin, tukiprosesseihin ja tietoresursseihin, niiden kriittisyyden mukaan. Tämä riskiarviointi tulee tehdä ja dokumentoida vuosittain tai tarvittaessa useammin. Tällaisia riskiarviointeja tulee tehdä myös kaikista merkittävistä muutoksista infrastruktuurissa, prosesseissa tai menettelyissä, jotka vaikuttava liiketoimintoihin, tukiprosesseihin tai

tietoresursseihin, ja finanssilaitoksen voimassa olevaa riskiarviota tulee päivittää niiden perusteella.

21. Finanssilaitosten tulee varmistaa, että ne seuraavat jatkuvasti liiketoimintojensa, tukiprosessiensa ja tietoresurssiensa kannalta merkityksellisiä uhkia ja haavoittuvuuksia, ja niiden tulee tarkastaa säännöllisesti niihin vaikuttavat riskiskenaariot.

1.3.4. Riskien vähentäminen

22. Finanssilaitosten tulee riskiarviointien perusteella määrittää, mitä toimenpiteitä tarvitaan vähentämään havaitut ICT- ja turvallisuusriskit hyväksyttäville tasoille ja onko nykyisiä liiketoimintaprosesseja, kontrolleja, ICT-järjestelmiä ja -palveluja muutettava. Finanssilaitosten tulee ottaa huomioon aika, joka näiden muutosten toteuttamiseen tarvitaan, sekä aika, joka tarvitaan sellaisten asianmukaisten väliaikaisten vähentämiskeinojen toteuttamiseen, joilla vähennetään ICT- ja turvallisuusriskejä, jotta ne pysyisivät finanssilaitosten ICT- ja turvallisuusriskejä koskevan riskinottohalun rajoissa.

23. Finanssilaitosten tulee määrittää ja toteutettava toimenpiteitä, joilla lievennetään yksilöityjä ICT- ja turvallisuusriskejä ja suojellaan tietoresursseja niiden luokituksen mukaisesti.

1.3.5. Raportointi

24. Finanssilaitosten tulee raportoida riskiarvioinnin tuloksista ylimmälle hallintoelimelle selkeästi ja asianmukaisen ajan kuluessa. Tällainen raportointi ei vaikuta maksupalveluntarjoajien velvoitteeseen toimittaa toimivaltaisille viranomaisille kattava ja päivitetty riskiarviointi direktiivin (EU) 2015/2366 95 artiklan 2 kohdan mukaisesti.

1.3.6. Tarkastus

25. Tarkastajien, joilla on riittävä tietämys, osaaminen ja asiantuntemus ICT- ja turvallisuusriskeistä ja maksuista (maksupalveluntarjoajien osalta), tulee tarkastaa finanssilaitoksen ICT- ja turvallisuusriskejä koskeva hallinto, järjestelmät ja prosessit määräajoin, jotta niiden tehokkuudesta voitaisiin antaa riippumaton varmistus ylimmälle hallintoelimelle. Tarkastajien tulee olla riippumattomia finanssilaitoksessa tai finanssilaitoksesta. Kyseisten tarkastusten tiheyden ja kohteen tulee olla oikeassa suhteessa asiaankuuluviin ICT- ja turvallisuusriskeihin.

26. Finanssilaitoksen ylimmän hallintoelimen tulee hyväksyä tarkastussuunnitelma, myös ICT-tarkastukset ja kaikki niihin tehtävät olennaiset muutokset. Tarkastussuunnitelman ja sen toteuttamisen, myös tarkastustiheyden, tulee perustua finanssilaitokselle ominaisiin ICT- ja turvallisuusriskeihin ja olla oikeassa suhteessa niihin. Suunnitelmaa tulee päivittää säännöllisesti.

27. Tulee laatia virallinen seurantaprosessi, joka sisältää myös säännöt ICT-tarkastuksen kriittisten havaintojen todentamiseksi ja korjaamiseksi mahdollisimman nopeasti.

1.4. Tietoturva

1.4.1. Tietoturvapolitiikka

28. Finanssilaitosten tulee laatia ja dokumentoida tietoturvapolitiikka, jossa tulee määrittää korkean tason periaatteet ja säännöt finanssilaitosten ja niiden asiakkaiden tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi. Maksupalveluntarjoajien osalta tämä käytäntö yksilöidään direktiivin (EU) 2015/2366 5 artiklan 1 kohdan j alakohdan mukaisesti annettavassa turvapolitiikka-asiakirjassa. Tietoturvapolitiikan tulee olla finanssilaitoksen tietoturvatavoitteiden mukaista ja perustua riskinarviointiprosessin asiaankuuluviin tuloksiin. Ylimmän hallintoelimen tulee hyväksyä kyseinen politiikka.

29. Politiikan tulee sisältää kuvaus tietoturvahallinnan keskeisistä tehtävistä ja vastuista, ja siinä tulee esittää henkilöstöä ja palveluntarjojia koskevat vaatimukset, prosessit ja teknologia tietoturvan osalta ja todeta, että kaikilla tasoilla henkilöstöllä ja palveluntarjoajilla on vastuita finanssilaitosten tietoturvan varmistamisessa. Politiikan tulee varmistaa finanssilaitosten kriittisten loogisten ja fyysisten varojen ja resurssien sekä arkaluonteisten tietojen luottamuksellisuus, eheys ja saatavuus niin talletettuna, siirrossa kuin käytössäkin. Tietoturvapolitiikasta tulee tiedottaa finanssilaitoksen kaikille työntekijöille ja palveluntarjoajille.

30. Tietoturvapolitiikan perusteella finanssilaitosten tulee laatia ja ottaa käyttöön turvatoimenpiteet, joilla vähennetään ICT- ja turvallisuusriskejä, joille ne altistuvat. Näihin toimenpiteisiin tulee kuulua

    a) järjestäminen ja hallinto 10 ja 11 kohdan mukaisesti
    b) looginen turvallisuus (1.4.2 jakso)
    c) fyysinen turvallisuus (1.4.3 jakso)
    d) ICT-operaatioiden turvallisuus (1.4.4 jakso)
    e) turvallisuusvalvonta (1.4.5 jakso)
    f) tietoturvatarkastukset, -arviointi ja -testaus (1.4.6 jakso)
    g) tietoturvakoulutus ja -tietoisuus (1.4.7 jakso)

1.4.2. Looginen turvallisuus

31. Finanssilaitosten tulee määrittää, dokumentoida ja ottaa käyttöön loogisen pääsynhallinnan menettelyitä (identiteetin ja pääsyn hallinta). Nämä menettelyt tulee toteuttaa ja niitä tulee valvoa ja seurata, ja ne tulee tarkastaa määräajoin. Menettelyihin tulee myös kuulua poikkeamien seurannan kontrollit. Menettelyissä tulee toteuttaa vähintään seuraavat tekijät (termi ”käyttäjä” tarkoittaa myös teknisiä käyttäjiä):

    (a) **Tiedonsaantitarve, pienimmän valtuuden periaate ja tehtävien erillään pitäminen:** Finanssilaitosten tulee hallinnoida tietoresursseja ja niiden tukijärjestelmiä koskevia käyttöoikeuksia tiedonsaantitarpeen perusteella, etäkäyttö mukaan lukien. Käyttäjille tulee antaa vähimmäiskäyttöoikeudet, joita heidän tehtäviensä suorittamiseen tarkkaan ottaen tarvitaan (’least privilege’, pienimmän valtuuden periaate), jotta voitaisiin estää

perusteeton pääsy suuriin tietomääriin tai estää sellaisten käyttöoikeusyhdistelmien myöntäminen, joita voidaan käyttää kontrollien kiertämiseen (’segregation of duties’, tehtävien erillään pitämisen periaate).

(b) **Käyttäjän vastuu:** Finanssilaitosten tulee rajoittaa mahdollisimman paljon yleisten ja yhteisten käyttäjätilien käyttöä ja varmistaa, että käyttäjät voidaan tunnistaa ICT-järjestelmissä suoritettujen toimien osalta.

(c) **Erityiskäyttöoikeudet:** Finanssilaitosten tulee ottaa käyttöön vahvoja kontrolleja erityiskäyttöoikeuksien valvontaan rajoittamalla tiukasti tilejä, joilla käyttöoikeudet ovat muita laajemmat (esim. ylläpitäjän tilit), ja valvoa niitä tiiviisti. Turvallisen viestinnän varmistamiseksi ja riskin pienentämiseksi hallintaoikeudellinen etäpääsy kriittisiin ICT-järjestelmiin tulee myöntää vain tarvepohjaisesti ja vahvojen tunnistusmenetelmien ollessa käytössä.

(d) **Käyttäjätoimintojen seuranta:** Vähintään kaikista erityiskäyttäjien tekemistä toimista tulee kerätä lokia ja niitä tulee valvoa. Käyttölokit tulee suojata luvattomalta muuttamiselta ja poistamiselta, ja niitä tulee säilyttää asiaankuuluva aika tunnistettujen liiketoimintojen, tukiprosessien ja tietoresurssien kriittisyyden perusteella 1.3.3 jakson mukaisesti, rajoittamatta kuitenkaan EU:n ja kansallisessa lainsäädännössä asetettuja säilytysvaatimuksia. Finanssilaitoksen tulee käyttää näitä tietoja helpottaakseen sellaisten poikkeavien toimien tunnistamista ja tutkintaa, jotka on havaittu palveluja tarjottaessa.

(e) **Pääsynhallinta:** Käyttöoikeudet tulee myöntää tai peruuttaa tai niitä tulee muuttaa nopeasti sellaisten etukäteen määritettyjen hyväksymismenettelyjen mukaisesti, joissa käytettävien tietojen liiketoiminnallinen omistaja (tietoresurssien omistaja) on mukana. Jos työsuhde päättyy, käyttöoikeudet tulee peruuttaa viipymättä.

(f) **Käyttöoikeuksien uudelleentarkistukset:** Käyttöoikeudet tulee tarkistaa määräajoin, jotta voitaisiin varmistaa, että käyttäjillä ei ole liiallisia oikeuksia ja että käyttöoikeudet peruutetaan, kun niitä ei enää tarvita.

(g) **Tunnistusmenetelmät:** Finanssilaitosten tulee valvoa, että tunnistusmenetelmät ovat riittävän vahvat, jotta voitaisiin varmistaa asianmukaisesti ja tehokkaasti käyttöoikeuksien hallintaperiaatteiden ja -menettelyjen noudattaminen. Tunnistusmenetelmien tulee olla oikeassa suhteessa käytettävien ICT-järjestelmien, tietojen tai prosessin kriittisyyteen. Tämän tulee sisältää ainakin monimutkaisia salasanoja tai tavallista vahvempia tunnistusmenetelmiä (kuten kaksivaiheinen tunnistus) asianomaisen riskin perusteella.

32. Elektroninen pääsy tietoihin ja ICT-järjestelmiin sovellusten avulla tulee rajoittaa minimiin, joka on tarpeen asiaankuuluvan palvelun tarjoamiseksi.

1.4.3. Fyysinen turvallisuus

33. Finanssilaitosten fyysistä turvallisuutta koskevat toimenpiteet tulee määrittää, dokumentoida ja ottaa käyttöön finanssilaitosten tilojen, konesalien ja arkaluonteisten alueiden suojaamiseksi luvattomalta pääsyltä ja ympäristövaaroilta.

34. Fyysinen pääsy ICT-järjestelmiin tulee sallia vain valtuutetuille henkilöille. Valtuudet tulee antaa vain henkilöiden tehtävien ja vastuiden mukaisesti ja vain asianmukaisesti koulutetuille ja valvotuille henkilöille. Fyysinen pääsy tulee tarkistaa määräajoin sen varmistamiseksi, että tarpeettomat käyttöoikeudet kumotaan viipymättä, kun niitä ei enää tarvita.

35. Ympäristövaaroilta suojaavien asianmukaisten toimenpiteiden tulee olla oikeassa suhteessa rakennusten merkitykseen ja kyseisissä rakennuksissa sijaitsevien operaatioiden tai ICT-järjestelmien kriittisyyteen nähden.

1.4.4. ICT-87operaatioiden turvallisuus

36. Finanssilaitosten tulee ottaa käyttöön menettelyitä, joilla estetään turvallisuusongelmat ICT-järjestelmissä ja -palveluissa, ja vähentää niiden vaikutusta ICT-palvelujen toimittamiseen. Näihin menettelyihin tulee kuulua seuraavat toimenpiteet:

    a) sellaisten mahdollisten haavoittuvuuksien tunnistaminen, jotka tulee arvioida ja korjata, varmistamalla, että ohjelmistot ja laitteistot ovat ajan tasalla, myös finanssilaitosten sisäisille ja ulkoisille käyttäjilleen tarjoamat ohjelmistot, ottamalla käyttöön kriittisiä turvallisuuskorjauksia tai toteuttamalla korvaavia kontrolleja
    b) kaikkien verkon komponenttien turvallisten konfiguroinnin perustasojen toteuttaminen
    c) verkon segmentoinnin, tietojen menettämisen ehkäisyjärjestelmien ja verkkoliikenteen salauksen toteuttaminen (tietoluokituksen mukaisesti)
    d) päätepisteiden, myös palvelimien, työasemien ja mobiililaitteiden suojan toteuttaminen; finanssilaitosten tulee arvioida, täyttävätkö päätepisteet niiden määrittämät turvallisuusvaatimukset ennen kuin niille myönnetään pääsy organisaation laajuiseen verkkoon
    e) sen varmistaminen, että käytössä on mekanismeja, joilla todennetaan ohjelmistojen, laitteistojen ja tietojen eheys
    f) talletettuna ja siirrossa olevien tietojen salaus (tietoluokituksen mukaisesti).

37. Finanssilaitosten tulee lisäksi määrittää jatkuvasti, vaikuttavatko nykyisen toimintaympäristön muutokset nykyisiin turvatoimenpiteisiin tai vaativatko ne muiden toimenpiteiden käyttöönottoa niihin kuuluvan riskin lieventämiseksi asianmukaisesti. Näiden muutosten tulee olla osa finanssilaitosten virallista muutoksenhallintaprosessia, jossa tulee varmistaa, että muutokset suunnitellaan, testataan, dokumentoidaan, valtuutetaan ja otetaan käyttöön asianmukaisesti.

1.4.5. Tietoturvatapahtumien monitorointi

38. Finanssilaitosten tulee laatia ja ottaa käyttöön käytännöt ja menettelyt, joilla havaitaan finanssilaitosten tietoturvaan mahdollisesti vaikuttavat poikkeavat toiminnot ja joilla voidaan reagoida näihin tapahtumiin asianmukaisesti. Finanssilaitosten tulee osana tätä jatkuvaa valvontaa ottaa käyttöön asianmukaiset ja tehokkaat valmiudet, joilla voidaan havaita fyysinen tai looginen tunkeutuminen sekä tietoresursseihin kohdistuneet luottamuksellisuuden, eheyden ja saatavuuden rikkomukset ja joilla voidaan raportoida niistä. Jatkuvien valvonta- ja havainnointiprosessien tulee kattaa seuraavat:

a) asiaan liittyvät sisäiset ja ulkoiset tekijät, mukaan lukien liiketoiminta ja hallinnolliset ICT-toiminnot
b) tapahtumat, joilla havaitaan kolmansien osapuolien tai muiden yhteisöjen toteuttama käyttöoikeuksien väärinkäyttö tai sisäinen käyttöoikeuksien väärinkäyttö
c) mahdolliset sisäiset ja ulkoiset uhat.

39. Finanssilaitosten tulee laatia ja ottaa käyttöön prosesseja ja organisaatiorakenteita voidakseen tunnistaa ja valvoa jatkuvasti turvallisuusuhkia, jotka voisivat vaikuttaa merkittävästi niiden kykyyn tarjota palveluja. Finanssilaitosten tulee seurata aktiivisesti tekniikan kehitystä varmistaakseen tietoisuutensa turvallisuusriskeistä. Finanssilaitosten tulee ottaa käyttöön havainnointitoimenpiteitä, jotta voitaisiin esimerkiksi tunnistaa mahdolliset tietovuodot, haitalliset koodit ja muut turvallisuusuhat sekä yleisesti tunnetut ohjelmisto- ja laitehaavoittuvuudet, ja niiden tulee tarkistaa vastaavat uudet turvallisuuspäivitykset.

40. Turvallisuusvalvontaprosesseilla tulee myös auttaa finanssilaitosta ymmärtämään operatiivisten poikkeamien tai turvapoikkeamien luonne, tunnistaa trendejä ja tukea organisaation tutkimuksia.

1.4.6. Tietoturvatarkastukset, -arviointi ja -testaus

41. Finanssilaitosten tulee tehdä erilaisia tietoturvatarkastuksia, -arviointeja ja -testauksia voidakseen varmistaa tieto- ja viestintäteknisten järjestelmiensä ja palvelujensa haavoittuvuuksien tehokkaan havaitsemisen. Finanssilaitokset voivat esimerkiksi tehdä puuteanalyysin tietoturvastandardien, vaatimustenmukaisuustarkastusten, tietojärjestelmien sisäisten ja ulkoisten tarkastusten tai fyysisen turvallisuuden tarkastusten perusteella. Laitoksen tulee myös ottaa huomioon hyvät käytännöt, kuten lähdekoodin tarkistukset, haavoittuvuusarvioinnit, tunkeutumistestit ja hyökkäysharjoitukset (red team exercises).

42. Finanssilaitosten tulee laatia ja ottaa käyttöön tietoturvan testauskehys, jossa validoidaan niiden tietoturvatoimenpiteiden vahvuus ja tehokkuus ja varmistetaan, että kehyksessä otetaan huomioon uhat ja haavoittuvuudet, jotka on havaittu uhkien seurannassa ja ICT- ja turvallisuusriskien arviointiprosessissa.

43. Tietoturvan testauskehyksellä tulee varmistaa, että

a) testeistä huolehtivat riippumattomat testaajat, joilla on riittävä tietämys, osaaminen ja asiantuntemus tietoturvatoimenpiteiden testaamisesta ja jotka eivät ole mukana tietoturvatoimenpiteiden kehittämisessä
b) testeihin kuuluu haavoittuvuuskartoituksia ja tunkeutumistestejä (myös uhkaan perustuvaa tunkeutumistestausta, kun se on tarpeen ja asianmukaista), joka on oikeassa suhteessa liiketoimintaprosesseissa ja -järjestelmissä määritetyn riskin tasoon nähden.

44. Finanssilaitosten tulee testata turvatoimenpiteitä jatkuvasti ja toistuvasti. Kaikkien kriittisten ICT-järjestelmien (17 kohta) osalta testit tulee tehdä vähintään vuosittain. Maksupalveluntarjoajien osalta ne ovat osa niiden tarjoamiin maksupalveluihin liittyvien turvallisuusriskien kattavaa arviointia toisen maksupalveludirektiivin 95 artiklan 2 kohdan

mukaisesti. Muut kuin kriittiset järjestelmät tulee testata säännöllisesti riskipohjaisella lähestymistavalla, mutta vähintään kolmen vuoden välein.

45. Finanssilaitosten tulee varmistaa, että turvallisuustoimenpiteet testataan, kun infrastruktuuriin, prosesseihin tai menettelyihin tulee muutoksia tai jos muutoksia tehdään merkittävien operatiivisten poikkeamien tai turvapoikkeamien vuoksi tai siksi, että julkaistaan uusia tai huomattavasti muuttuneita verkossa käytettäviä kriittisiä sovelluksia.

46. Finanssilaitosten tulee myöntää ja arvioida turvallisuustestien tuloksia ja päivittää turvatoimenpiteensä vastaavasti ja ilman tarpeetonta viivytystä kriittisten ICT-järjestelmien osalta.

47. Maksupalveluntarjoajien osalta testauskehyksen tulee sisältää myös turvatoimenpiteet, jotka ovat asiaankuuluvat 1) niiden maksupäätteiden ja laitteiden kannalta, joita käytetään maksupalvelujen tarjoamiseen, 2) niiden maksupäätteiden ja laitteiden kannalta, joita käytetään maksupalvelunkäyttäjän tunnistamiseen ja 3) niiden laitteiden ja ohjelmistojen kannalta, jotka maksupalveluntarjoaja tarjoaa maksupalvelunkäyttäjälle tunnistuskoodin luomiseksi/vastaanottamiseksi.

48. Testaaminen tulee havaittujen turvallisuusuhkien ja tehtyjen muutosten perusteella tehdä niin, että siihen sisältyvät asiaan liittyvien ja tunnettujen mahdollisten hyökkäysten skenaariot.

1.4.7. Tietoturvakoulutus ja -tietoisuus

49. Finanssilaitosten tulee laatia koulutusohjelma, myös määräaikaiset turvatietoisuusohjelmat, kaikille työntekijöille ja palveluntarjoajille sen varmistamiseksi, että heidät on koulutettu suorittamaan tehtävänsä ja vastuunsa asiaankuuluvien turvallisuuskäytäntöjen ja -menettelyjen mukaisesti, jolloin pienennetään inhimillisen virheen, varkauden, petoksen, väärinkäytön tai tappion vaaraa, ja puuttumaan tietoturvaan liittyviin riskeihin. Finanssilaitosten tulee varmistaa, että koulutusohjelmassa annetaan koulutusta kaikille työntekijöille ja palveluntarjoajille vähintään vuosittain.

1.5. ICT-operaatioiden hallinta

50. Finanssilaitosten tulee hallita ICT-operaatioitaan ylimmän hallintoelimen hyväksymien dokumentoitujen ja toteutettujen prosessien ja menettelyjen (joihin maksupalveluntarjoajien osalta kuuluvat toisen maksupalveludirektiiviin 5 artiklan 1 kohdan j alakohdan mukaiset turvapolitiikka-asiakirjat) mukaisesti. Näissä asiakirjoissa tulee määrittää, miten finanssilaitokset käyttävät, seuraavat ja valvovat ICT-järjestelmiään ja palveluitaan sekä dokumentoivat kriittiset ICT-operaatiot. Niiden avulla finanssilaitosten tulee pystyä pitämään ICT-resurssien luettelo ajan tasalla.

51. Finanssilaitosten tulee varmistaa, että niiden ICT-operaatioiden suorituskyky on niiden liiketoimintavaatimusten mukaista. Finanssilaitosten tulee pitää yllä ja mahdollisuuksien mukaan parantaa ICT-operaatioidensa tehokkuutta. Niiden tulee muun muassa pohtia, miten vähennetään manuaalisten tehtävien suorittamisesta johtuvia mahdollisia virheitä.

52. Finanssilaitosten tulee ottaa käyttöön kriittisten ICT-operaatioiden lokitus- ja seurantamenettelyt, jotta virheet voitaisiin havaita, analysoida ja korjata.

53. Finanssilaitosten tulee pitää yllä ajan tasalla olevaa luetteloa ICT-resursseistaan (myös ICT-järjestelmistä, verkkolaitteista, tietokannoista jne.). ICT-resurssien luetteloon tulee tallentaa ICT-resurssien konfiguraatio ja linkit, sekä ottaa huomioon keskinäiset riippuvuudet erilaisten ICT-resurssien välillä asianmukaisen konfiguraation ja muutoshallintaprosessin mahdollistamiseksi.

54. ICT-resurssien luettelon tulee olla riittävän yksityiskohtainen, jotta ICT-resurssi, sen sijainti, turvaluokitus ja omistajuus voitaisiin tunnistaa ripeästi. Resurssien väliset riippuvuudet tulee dokumentoida, mikä edesauttaa turvallisuuspoikkeamiin ja operatiivisiin poikkeamiin (myös kyberhyökkäyksiin) reagointia.

55. Finanssilaitosten tulee seurata ja hallita ICT-resurssien elämänkaaria, jotta voitaisiin varmistaa, että ne täyttävät jatkuvasti liiketoiminnan ja riskinhallinnan vaatimukset ja tukevat niitä. Finanssilaitosten tulee seurata, tukevatko niiden ulkoiset tai sisäiset alihankkijat ja kehittäjät niiden ICT-resursseja ja tehdäänkö kaikki asiaankuuluvat korjaukset ja päivitykset dokumentoitujen prosessien perusteella. Vanhentuneista tai tukea vailla olevista ICT-resursseista johtuvat riskit tulee arvioida ja niitä tulee vähentää.

56. Finanssilaitosten tulee ottaa käyttöön suorituskyvyn ja kapasiteetin suunnittelua ja seurantaa koskevat prosessit, jotta voitaisiin estää ja havaita ICT-järjestelmien merkittävät suorituskykyongelmat ja tieto- ja viestintätekniikan kapasiteettipuutteet ja reagoida niihin ajoissa.

57. Finanssilaitosten tulee määrittää ja ottaa käyttöön tietojen ja ICT-järjestelmien varmistus- ja palauttamismenettelyt, jotta voitaisiin varmistaa niiden tarvittavan toimintakunnon palauttaminen. Varmistusten laajuus ja tiheys tulee määrittää liiketoiminnan palauttamista koskevien vaatimusten ja tietojen ja ICT-järjestelmien kriittisyyden mukaisesti ja arvioida tehdyn riskiarvioinnin mukaisesti. Varmistus- ja palautusmenettelyt tulee testata määräajoin.

58. Finanssilaitosten tulee varmistaa, että tietojen ja ICT-järjestelmien varmistukset säilytetään suojatusti ja että ne ovat riittävän kaukana ensisijaisesta paikasta, jotta ne eivät altistuisi samoille riskeille.

3.5.1 ICT-poikkeamien ja ongelmien hallinta

59. Finanssilaitosten tulee laatia ja ottaa käyttöön poikkeamien ja ongelmien hallintaprosessi, jolla seurataan tieto- ja viestintätekniikan operatiivisia poikkeamia ja turvallisuuspoikkeamia ja kirjataan ne ja jonka avulla finanssilaitokset voivat häiriötapauksessa jatkaa kriittisiä liiketoimintoja ja -prosesseja tai palauttaa ne mahdollisimman nopeasti. Finanssilaitosten tulee määrittää asianmukaiset kriteerit ja kynnysarvot sille, että tapahtumat luokitellaan operatiivisiksi poikkeamiksi tai turvapoikkeamiksi, näiden ohjeiden Määritelmät-jakson mukaisesti, sekä varhaiset varoitusmerkit, jotka antavat hälytyksen, joiden avulla nämä poikkeamat voidaan havaita varhain. Tällaiset kriteerit ja kynnysarvot eivät maksupalveluntarjoajien osalta vaikuta merkittävien poikkeamien luokitukseen toisen

maksupalveludirektiivin 96 artiklan ja direktiivin (EU) 2015/2366 (PSD2) mukaisesta merkittävien häiriöiden raportoinnista annettujen ohjeiden (EBA/GL/2017/10) mukaisesti.

60. Jotta haitallisten tapahtumien vaikutusta voitaisiin vähentää ja palauttaa toimintakunto mahdollisimman nopeasti, finanssilaitosten tulee laatia asianmukaiset prosessit ja organisaatiorakenteet, joilla varmistetaan operatiivisten poikkeamien ja turvallisuuspoikkeamien johdonmukainen ja yhdennetty valvonta, käsittely ja seuranta ja taataan, että perimmäiset syyt määritetään ja poistetaan estämään toistuvien poikkeamien ilmeneminen. Poikkeamien ja ongelmien hallintaprosessissa tulee vahvistaa

    a) menettelyt poikkeamien havaitsemiseksi, jäljittämiseksi, kirjaamiseksi, ryhmittelemiseksi ja luokittelemiseksi ensisijaisuuden mukaan liiketoimintaa koskevan kriittisyyden perusteella
    b) tehtävät ja vastuut eri poikkeamaskenaarioissa (esim. virheet, toimintahäiriöt, kyberhyökkäykset)
    c) ongelmien hallintamenettelyt yhden tai useamman poikkeaman takana olevan perimmäisen syyn havaitsemiseksi, analysoimiseksi ja ratkaisemiseksi – finanssilaitoksen tulee analysoida finanssilaitokseen todennäköisesti vaikuttavat operatiiviset poikkeamat tai turvapoikkeamat, jotka on määritetty tai jotka ovat ilmenneet organisaatiossa ja/tai sen ulkopuolella, ja ottaa huomioon näistä analyyseista opitut keskeiset asiat ja päivittää turvatoimenpiteitä sen mukaisesti
    d) tehokkaat sisäiset viestintäsuunnitelmat, myös poikkeamailmoitukset ja eskalointimenettelyt, jotka kattavat myös turvallisuuteen liittyvät asiakasvalitukset ja joilla varmistetaan, että
        i) poikkeamista, joilla on mahdollisesti suuri haitallinen vaikutus kriittisiin ICT-järjestelmiin ja -palveluihin, raportoidaan asiaankuuluvalle toimivalle johdolle ja toimivalle ICT-johdolle
        ii) ylimmälle hallintoelimelle ilmoitetaan tapauskohtaisesti merkittävistä poikkeamista ja ilmoitetaan ainakin vaikutuksesta, reagoinnista ja lisäkontrolleista, jotka tulee määrittää poikkeamien vuoksi
    e) poikkeamia koskevat menettelyt, jotta voitaisiin vähentää poikkeamienvaikutuksia ja varmistaa, että palvelu saadaan toimintakuntoon ja turvalliseksi mahdollisimman nopeasti
    f) erityiset ulkoiset viestintäsuunnitelmat kriittisille liiketoiminnoille ja prosesseille, jotta voitaisiin
        i) tehdä yhteistyötä asiaankuuluvien sidosryhmien kanssa, jotta poikkeamaan voitaisiin reagoida ja palautua siitä tehokkaasti
        ii) antaa ajantasaista tietoa ulkoisille osapuolille (esim. asiakkaille, muille markkinaosapuolille, valvontaviranomaiselle) tarpeen mukaan ja sovellettavan lainsäädännön mukaisesti.

1.6. ICT-projektit ja muutoshallinta

1.6.1. ICT-projektien hallinta

61. Finanssilaitoksen tulee ottaa käyttöön hankkeen ja/tai projektin hallintaprosessi, jossa määritetään tehtävät, vastuut ja velvollisuudet, jotta ICT-strategian toteuttamista voitaisiin tukea tehokkaasti.

62. Finanssilaitoksen tulee asianmukaisesti valvoa ja vähentää riskejä, jotka johtuvat niiden ICT-projektisalkusta (hankkeiden hallinta), ja ottaa myös huomioon riskit, jotka voivat johtua keskinäisistä riippuvuuksista eri projektien välillä sekä useiden projektien riippuvuudesta samoista resursseista ja/tai asiantuntemuksesta.

63. Finanssilaitoksen tulee laatia ja ottaa käyttöön ICT-projektinhallinnan toimintalinjoja, jotka sisältävät ainakin

    a) projektin tavoitteet
    b) tehtävät ja vastuut
    c) projektin riskiarvioinnin
    d) projektisuunnitelman, aikataulun ja vaiheet
    e) tärkeimmät välitavoitteet
    f) muutoksenhallintavaatimukset.

64. ICT-projektin hallintapolitiikalla tulee varmistaa, että tietoturvavaatimukset analysoi ja hyväksyy toiminto, joka on riippumaton kehitystoiminnosta.

65. Finanssilaitoksen tulee varmistaa, että kaikki alat, joihin ICT-projekti vaikuttaa, ovat edustettuina projektiryhmässä ja että projektiryhmässä on vaadittavaa tietämystä turvallisen ja onnistuneen projektin toteuttamisen varmistamiseksi.

66. ICT-projektin laatimisesta ja edistymisestä sekä niihin liittyvistä riskeistä tulee raportoida ylimmälle hallintoelimelle yksittäin tai kootusti ICT-projektin merkityksen ja koon mukaan säännöllisesti ja tarpeen mukaan tapauskohtaisesti. Finanssilaitosten tulee sisällyttää projektiriski riskinhallintakehykseensä.

1.6.2. ICT-järjestelmien hankinta ja kehittäminen

67. Finanssilaitosten tulee kehittää ja ottaa käyttöön prosessi, jolla hallitaan ICT-järjestelmien hankintaa, kehittämistä ja ylläpitoa. Tämä prosessi tulee suunnitella riskipohjaista lähestymistapaa käyttämällä.

68. Finanssilaitoksen tulee varmistaa, että ennen ICT-järjestelmien hankinnan tai kehittämisen toteuttamista asiaankuuluva liiketoimintajohto määrittelee selkeästi ja hyväksyy toiminnalliset ja ei-toiminnalliset vaatimukset (mukaan lukien tietoturvavaatimukset).

69. Finanssilaitoksen tulee varmistaa, että käytössä on toimenpiteitä, joilla vähennetään ICT-järjestelmien tahattoman muuttamisen tai tahallisen manipulaation riskiä kehittämisen ja toteuttamisen aikana tuotantoympäristössä.

70. Finanssilaitoksilla tulee olla käytössä menetelmä ICT-järjestelmien testaamiseen ja hyväksymiseen ennen niiden käyttöönottoa. Menetelmässä tulee huomioida liiketoimintaprosessien ja resurssien kriittisyys. Testauksella tulee varmistaa, että uudet ICT-järjestelmät toimivat suunnitellusti. Niiden tulee myös käyttää testiympäristöjä, jotka vastaavat riittävästi tuotantoympäristöä.

71. Finanssilaitosten tulee testata ICT-järjestelmiä ja -palveluja sekä tietoturvatoimenpiteitä mahdollisten turvallisuusheikkouksien, -loukkauksien ja -poikkeamien tunnistamiseksi.

72. Finanssilaitosten tulee ottaa käyttöön erillisiä ICT-ympäristöjä, jotta voitaisiin varmistaa asianmukaisesti tehtävien erillään pitäminen ja vähentää todentamattomien muutosten vaikutusta tuotantojärjestelmiin. Finanssilaitoksen tulee erityisesti varmistaa tuotantoympäristöjen pitäminen erillään kehittämisestä, testaamisesta ja muista ei-tuotantoympäristöistä. Finanssilaitoksen tulee varmistaa tuotantotietojen eheys ja luottamuksellisuus ei-tuotantoympäristöissä. Tuotantotietojen käyttö rajataan valtuutettuihin käyttäjiin.

73. Finanssilaitosten tulee ottaa käyttöön toimenpiteitä, joilla suojataan sisäisesti kehitettävien ICT-järjestelmien lähdekoodin luotettavuutta. Niiden tulee myös dokumentoida ICT-järjestelmien kehitys, toteuttaminen, toiminta ja/tai konfiguraatio kattavasti, jotta voitaisiin vähentää mahdollista tarpeetonta riippuvuutta alan asiantuntijoista. ICT-järjestelmien dokumentoinnin tulee soveltuvin osin sisältää ainakin käyttäjädokumentaatio, teknisen järjestelmän dokumentaatio ja toimintamenettelyt.

74. ICT-järjestelmien hankintaa ja kehittämistä koskevia finanssilaitoksen prosesseja tulee myös soveltaa ICT-järjestelmiin, joita liiketoiminnon loppukäyttäjät kehittävät ja hallinnoivat ICT-organisaation ulkopuolella (esim. loppukäyttäjän sovellukset) käyttämällä riskipohjaista lähestymistapaa. Finanssilaitoksen tulee pitää yllä rekisteriä näistä sovelluksista, joilla tuetaan kriittisiä liiketoimintoja tai liiketoimintaprosesseja.

1.6.3. ICT-muutoksenhallinta

75. Finanssilaitosten tulee laatia ja ottaa käyttöön ICT-muutoksenhallintaprosessi sen varmistamiseksi, että kaikki ICT-järjestelmien muutokset rekisteröidään, testataan, arvioidaan, hyväksytään, toteutetaan ja todennetaan hallitusti. Finanssilaitosten tulee käsitellä muutoksia hätätilanteiden aikana (eli muutoksia, jotka on otettava käyttöön mahdollisimman pian) riittävät varotoimet takaavia menettelyjä noudattaen.

76. Finanssilaitosten tulee määrittää, vaikuttavatko nykyisen toimintaympäristön muutokset nykyisiin turvatoimenpiteisiin tai vaativatko ne muiden toimenpiteiden käyttöönottoa niihin kuuluvien riskien vähentämiseksi. Näiden muutosten tulee noudattaa finanssilaitosten virallista muutoksenhallintaprosessia.

1.7. Liiketoiminnan jatkuvuuden hallinta

77. Finanssilaitosten tulee laatia vakaata liiketoiminnan jatkuvuuden hallintaa koskeva prosessi, jotta voitaisiin maksimoida niiden valmiudet tarjota palveluja jatkuvasti ja rajoittaa tappioita

liiketoiminnan vakavien häiriöiden varalta direktiivin 2013/36/EU 85 artiklan 2 kohdan ja Euroopan pankkiviranomaisen hallinnosta ja ohjauksesta antamien ohjeiden (EBA/GL/2017/11) VI osaston mukaisesti.

1.7.1. Liiketoiminnan vaikutusanalyysi (business impact analysis)

78. Osana vakaata liiketoiminnan jatkuvuuden hallintaa finanssilaitosten tulee tehdä liiketoiminnan vaikutusanalyysi analysoimalla altistumistaan liiketoiminnan vakaville häiriöille ja arvioimalla niiden mahdollisia vaikutuksia (myös luottamuksellisuuteen, eheyteen ja saatavuuteen) määrällisesti ja laadullisesti, käyttämällä sisäisiä ja/tai ulkoisia tietoja (esim. liiketoimintaprosessin kannalta merkityksellisiä ulkopuolisen palveluntarjoajan tietoja tai liiketoiminnan vaikutusanalyysin kannalta mahdollisesti merkittäviä julkisesti saatavilla olevia tietoja) ja tekemällä skenaarioanalyysi. Liiketoiminnan vaikutusanalyysissa tulee myös ottaa huomioon tunnistettujen ja luokiteltujen liiketoimintojen, tukiprosessien, kolmansien osapuolten ja tietoresurssien kriittisyys sekä niiden keskinäiset riippuvuudet 1.3.3 jakson mukaisesti.

79. Finanssilaitosten tulee varmistaa, että niiden ICT-järjestelmät ja -palvelut on suunniteltu ja mukautettu liiketoiminnan vaikutusanalyysin mukaisesti esimerkiksi siten, että tietyillä kriittisillä komponenteilla on varajärjestelmä, joka estää kyseisiin komponentteihin vaikuttavien tapahtumien aiheuttamat häiriöt.

1.7.2. Liiketoiminnan jatkuvuussuunnittelu

80. Finanssilaitosten tulee laatia liiketoiminnan vaikutusanalyysiensa perusteella suunnitelmia, joilla varmistetaan liiketoiminnan jatkuvuus (liiketoiminnan jatkuvuussuunnitelmat) ja jotka niiden ylimpien hallintoelinten tulee dokumentoida ja hyväksyä. Suunnitelmissa tulee erityisesti ottaa huomioon riskit, jotka voivat vaikuttaa haitallisesti ICT-järjestelmiin ja -palveluihin. Suunnitelmien tulee tukea tavoitteita siten, että ne suojaavat niiden liiketoimintojen, tukiprosessien ja tietoresurssien luottamuksellisuuden, eheyden ja saatavuuden ja tarvittaessa palauttavat ne. Finanssilaitosten tulee koordinoida kyseisten suunnitelmien laadintaa tarvittaessa asiaankuuluvien sisäisten ja ulkoisten sidosryhmien kanssa.

81. Finanssilaitosten tulee ottaa liiketoiminnan jatkuvuussuunnitelmat käyttöön sen varmistamiseksi, että ne voivat reagoida asianmukaisesti mahdollisiin häiriöskenaarioihin ja että ne pystyvät palauttamaan kriittisten liiketoimintojensa toimintakunnon häiriöiden jälkeen toipumisajan (RTO, Recovery Time Objective, enimmäisaika, jossa järjestelmä tai prosessi on palautettava häiriön jälkeen) ja palautuspistetavoitteessa (RPO, Recovery Point Objective, enimmäisaika, jolta tiedot voidaan menettää häiriötilanteessa). Mikäli kyse on vakavasta liiketoiminnan häiriöstä, jonka vuoksi aletaan soveltaa erityisiä liiketoiminnan jatkuvuussuunnitelmia, finanssilaitosten tulee asettaa liiketoiminnan jatkuvuussuunnitelmat tärkeysjärjestykseen käyttämällä riskipohjaista lähestymistapaa, joka voi perustua 1.3.3 jaksossa tarkoitettuihin riskiarviointeihin. Maksupalveluntarjoajan osalta tähän voi kuulua

esimerkiksi kriittisten tapahtumien jatkokäsittelyn helpottaminen samalla, kun korjaustoimia jatketaan.

82. Finanssilaitoksen tulee ottaa liiketoiminnan jatkuvuussuunnitelmassaan huomioon erilaiset skenaariot, joille se voi altistua, mukaan lukien äärimmäiset mutta uskottavilta tuntuvat skenaariot, muun muassa kyberhyökkäysskenaariot, sekä arvioida kyseisten skenaarioiden mahdollinen vaikutus. Näiden skenaarioiden perusteella finanssilaitoksen tulee kuvata, miten ICT- järjestelmien ja palvelujen jatkuvuus sekä finanssilaitosten tietoturva varmistetaan.

1.7.3. Toipumissuunnitelmat

83. Liiketoiminnan vaikutusanalyysin (78 kohta) ja uskottavilta tuntuvien skenaarioiden (82 kohta) perusteella finanssilaitosten tulee laatia toipumissuunnitelmat. Näissä suunnitelmissa tulee yksilöidä, minkä ehtojen perusteella suunnitelma otetaan käyttöön ja mihin toimiin olisi ryhdyttävä, jotta varmistettaisiin ainakin finanssilaitosten kriittisten ICT-järjestelmien ja -palvelujen saatavuus, jatkuvuus ja toimintakunnon palauttaminen. Toipumissuunnitelmien tavoitteena tulee olla finanssilaitoksen toimintojen toipumistavoitteiden täyttäminen.

84. Toipumissuunnitelmissa tulee ottaa huomioon sekä lyhyt- että pitkäaikaiset toipumisvaihtoehdot. Suunnitelmilta edellytetään seuraavaa:

    a) Niissä tulee keskittyä kriittisten liiketoimintojen, tukiprosessien ja tietoresurssien sekä niiden keskinäisten riippuvuuksien palauttamiseen, jotta vältettäisiin haitallisia vaikutuksia finanssilaitosten toimintaan ja finanssijärjestelmään, muun muassa maksujärjestelmiin ja maksujärjestelmien käyttäjiin, ja varmistettaisiin odottavien maksutapahtumien toteuttaminen.
    b) Ne tulee dokumentoida ja antaa liiketoiminta- ja tukiyksiköiden saataville ja niiden tulee olla heti käytettävissä hätätilanteessa.
    c) Niitä tulee päivittää sen mukaisesti, mitä on opittu aiemmista häiriöistä, uusista tunnistetuista riskeistä ja uhista sekä muuttuneista toipumistavoitteista ja prioriteeteista.

85. Suunnitelmissa tulee myös ottaa huomioon muita vaihtoehtoja, jos toipuminen ei ole toteuttamiskelpoista lyhyellä aikavälillä kustannusten, riskien, logistiikan ja ennakoimattomien olosuhteiden vuoksi.

86. Toipumissuunnitelmien osana finanssilaitoksen tulee myös harkita ja ottaa käyttöön jatkuvuustoimenpiteitä, joilla vähennetään sellaisten ulkopuolisten palveluntarjoajien häiriöitä, joiden merkitys on keskeinen finanssilaitoksen ICT-palvelun jatkuvuudelle (Euroopan pankkiviranomaisen ulkoistamista koskevien ohjeiden (EBA/GL/2019/02) mukaisesti) liiketoiminnan jatkuvuussuunnitelmien osalta.

1.7.4. Suunnitelmien testaus

87. Finanssilaitosten tulee testata liiketoiminnan jatkuvuussuunnitelmiaan määräajoin. Finanssilaitosten tulee erityisesti varmistaa, että niiden kriittisten liiketoimintojen, tukiprosessien, tietoresurssien ja niiden keskinäisten riippuvuuksien liiketoiminnan

jatkuvuussuunnitelmia (tarvittaessa myös kolmansien osapuolten tarjoamia) testataan vähintään vuosittain 89 kohdan mukaisesti.

88. Liiketoiminnan jatkuvuussuunnitelmia tulee päivittää vähintään vuosittain testitulosten, nykyisten uhkatietojen ja aiemmista tapahtumista opitun perusteella. Myös kaikki muutokset toipumistavoitteisiin (myös palautusaikatavoitteisiin (RTO) ja palautuspistetavoitteisiin (RPO) ja/tai muutokset liiketoimintoihin, tukiprosesseihin ja tietoresursseihin tulee tarvittaessa ottaa huomioon liiketoiminnan jatkuvuussuunnitelmien päivittämisen perustana.

89. Finanssilaitosten liiketoiminnan jatkuvuussuunnitelmien testauksessa tulee osoittaa, että niillä pystytään säilyttämään niitä koskevien liiketoimintojen elinkelpoisuus siihen asti, että kriittisten toimintojen toimintakyky palautetaan. Niiden tulee erityisesti

    a) sisältää riittävä määrä vakavien mutta uskottavilta tuntuvien skenaarioiden testausta, myös niiden, jotka otetaan huomioon liiketoiminnan jatkuvuussuunnitelmien kehittämisessä (sekä tarvittaessa kolmansien osapuolien tarjoamien palvelujen testaus); tähän tulee kuulua kriittisten liiketoimintojen, tukiprosessien ja tietoresurssien siirtäminen palautumisympäristöön ja sen osoittaminen, että ne voivat toimia tällä tavalla riittävän edustavan ajan ja että normaali toiminta voidaan palauttaa jälkeenpäin
    b) olla suunniteltu haastamaan oletukset, joihin liiketoiminnan jatkuvuuden suunnitelmat nojaavat, mukaan lukien hallinnointijärjestelyt ja kriisiviestintäsuunnitelmat, ja
    c) sisältää menettelyt, joilla todennetaan finanssilaitosten työntekijöiden ja palveluntarjoajien sekä ICT-järjestelmien ja -palvelujen valmius reagoida asianmukaisesti 89 kohdan a alakohdassa määritettyihin skenaarioihin.

90. Testitulokset tulee dokumentoida, ja kaikki testeistä johtuvat havaitut puutteet tulee analysoida, käsitellä ja raportoida ylimmälle hallintoelimelle.

1.7.5. Kriisiviestintä

91. Häiriö- tai hätätilanteessa ja liiketoiminnan jatkuvuussuunnitelmien käyttöönoton aikana finanssilaitosten tulee varmistaa, että niillä on käytössään tehokkaat kriisiviestintämenettelyt, jotta kaikille asiaankuuluville sisäisille ja ulkoisille sidosryhmille, myös toimivaltaisille viranomaisille, kun sitä edellytetään kansallisessa lainsäädännössä, sekä asiaankuuluville palveluntarjoajille (ulkoistamisen tarjoajat, konserniryhmän yksiköt tai kolmannet osapuolet) tiedotettaisiin hyvissä ajoin ja asianmukaisella tavalla.

1.8. Ohje 9: Maksupalvelunkäyttäjän liittyvien suhteiden hallinta

92. Maksupalveluntarjoajien tulee laatia ja ottaa käyttöön prosessit, joilla parannetaan maksupalvelunkäyttäjien tietoisuutta maksupalveluihin liittyvistä turvallisuusriskeistä, tarjoamalla maksupalvelunkäyttäjille apua ja neuvontaa.

93. Maksupalvelunkäyttäjille tarjottu apu ja neuvonta tulee päivittää uusien uhkien ja haavoittuvuuksien mukaan, ja muutoksista tulisi kertoa maksupalvelunkäyttäjälle.

94. Jos tuotteen toimivuus sen sallii, maksupalveluntarjoajien tulee sallia se, että maksupalvelunkäyttäjät voivat poistaa käytöstä tietyt maksupalveluntarjoajan maksupalvelunkäyttäjälle tarjoamiin maksupalveluihin liittyvät maksutoiminnot.

95. Jos maksupalveluntarjoaja on direktiivin (EU) 2015/2366 artiklan 68 kohdan 1 mukaisesti sopinut maksajan kanssa käyttörajoista tietyllä maksuvälineellä toteutettujen maksutapahtumien osalta, maksupalveluntarjoajan tulee tarjota maksajalle mahdollisuus muokata näitä rajoja suurimpaan sovittuun rajaan asti.

96. Maksupalveluntarjoajien tulee tarjota maksupalvelunkäyttäjille mahdollisuus saada hälytyksiä käynnistetyistä maksutapahtumista ja/tai maksutapahtumien epäonnistuneista käynnistysyrityksistä, jotta käyttäjät voisivat tunnistaa tiliensä petollisen tai haitallisen käytön.

97. Maksupalveluntarjoajien tulee pitää maksupalvelunkäyttäjät ajan tasalla sellaisten turvatoimenpiteiden päivityksistä, jotka vaikuttavat maksupalvelunkäyttäjiin maksupalvelujen tarjoamisen osalta.

98. Maksupalveluntarjoajien tulee tarjota maksupalvelunkäyttäjille apua kaikissa kysymyksissä, tukipyynnöissä ja poikkeamailmoituksissa tai ongelmissa, jotka koskevat maksupalveluihin liittyviä turvallisuusasioita. Maksupalvelunkäyttäjille tulee tiedottaa asianmukaisesti siitä, miten kyseistä apua saa.