Määräykset ja ohjeet 8/2014

Operatiivisen riskin hallinta rahoitussektorin valvottavissa

Dnro
FIVA 8/01.00/2014

Antopäivä
4.11.2014

Voimaantulopäivä
1.2.2015

FINANSSIVALVONTA
puh. 09 183 51
faksi 09 183 5328
etunimi.sukunimi@finanssivalvonta.fi
www.finanssivalvonta.fi

Lisätietoja
Taloudellinen analyysi ja operatiiviset riskit/Operatiiviset riskit

FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

Määräysten ja ohjeiden oikeudellinen luonne

Määräykset

Finanssivalvonnan määräys- ja ohjekokoelmassa ”Määräys”-otsikon alla esitetään Finanssivalvonnan antamat määräykset. Määräykset ovat velvoittavia oikeussääntöjä, joita on noudatettava.

Finanssivalvonta antaa määräyksiä ainoastaan määräyksenantoon valtuuttavan lain säännöksen nojalla ja sen asettamissa rajoissa.

Ohjeet

Finanssivalvonnan määräys- ja ohjekokoelmassa ”Ohje”-otsikon alla esitetään Finanssivalvonnan tulkintoja lainsäädännön tai muun velvoittavan sääntelyn sisällöstä.

”Ohje”-otsikon alla on lisäksi suosituksia ja muita toimintaohjeita, jotka eivät ole velvoittavia. Ohjeissa on myös kansainvälisten ohjeiden ja suositusten noudattamista koskevat Finanssivalvonnan suositukset.

Ohjeen kirjoitustavasta ilmenee, milloin kyseessä on tulkinta ja milloin suositus tai muu toimintaohje. Ohjeiden kirjoitustapaa sekä määräysten ja ohjeiden oikeudellista luonnetta on selvitetty tarkemmin Finanssivalvonnan verkkopalvelussa.

Finanssivalvonta.fi > Sääntely > Määräys- ja ohjekokoelma > Uusi määräyskokoelma

Sisällysluettelo

1 Soveltamisala ja määritelmät

1.1 Riskienhallinta

Näiden määräysten ja ohjeiden lukuja 4 – 7, 8.2., 9.1 ja 9.2 sovelletaan seuraaviin Finanssivalvonnasta annetussa laissa tarkoitettuihin valvottaviin: *(Annettu 29.1.2018, voimaan 1.3.2018*)

- luottolaitokset
- kolmannen maan luottolaitosten Suomessa olevat sivuliikkeet
- sijoituspalveluyritykset, joihin sovelletaan sijoituspalvelulain 6 luvun 2 §:n mukaisesti luottolaitostoiminnasta annetun lain 9,10 ja 11 luvun säännöksiä
- rahastoyhtiöt, jotka harjoittavat sijoitusrahastorahastolain 5 §:n 2 momentissa tarkoitettua toimintaa
- vaihtoehtorahastojen hoitajat, jotka tarjoavat sijoituspalveluja
- luottolaitoksen ja sijoituspalveluyrityksen omistusyhteisöt sekä rahoitus- ja vakuutusryhmittymien valvonnasta annetussa laissa tarkoitetut ryhmittymän omistusyhteisöt
- talletuspankkien yhteenliittymien keskusyhteisöt
- maksulaitokset

Näiden määräysten ja ohjeiden lukuja 4 – 6 ja 8.2. sovelletaan seuraavaan valvottavaan:

- pörssi

Lisäksi Finanssivalvonta suosittaa, että Suomessa olevat kolmansien maiden sijoituspalveluyritysten sivuliikkeet noudattaisivat näiden määräysten ja ohjeiden lukuja 4 – 7. 8.2, 9.1 ja 9.2. *(Annettu 29.1.2018, voimaan 1.3.2018)*

Maksujärjestelmiä koskevaa lukua 7 sovelletaan maksujenvälitystä harjoittaviin valvottaviin.

Maksupalveluja ilman toimilupaa tarjoaviin henkilöihin, mukaan lukien tilitietopalvelujen tarjoajat, sovelletaan lukuja 7 ja 9.1, joita sovelletaan kyseisissä luvuissa tarkemmin esitetyin osin. *(Annettu 29.1.2018, voimaan 1.3.2018)*

Lukua 9.3 (vuosittainen arvio maksupalvelujen operatiivisista ja turvallisuusriskeistä) sovelletaan maksupalveluja tarjoaviin valvottaviin ja maksupalveluja ilman toimilupaa tarjoaviin henkilöihin. (*Annettu 29.1.2018, voimaan 1.3.2018)*

1.2 Poikkeusoloihin varautuminen

Näiden määräysten ja ohjeiden lukua 8.3 sovelletaan seuraavassa lueteltuihin valvottaviin ja ulkomaisiin valvottaviin, jotka ovat velvollisia varautumaan valmiuslain (1552/2011) tarkoittamiin poikkeusoloihin.

- luottolaitokset
- maksulaitokset
- sijoituspalveluyritykset, jotka tarjoavat oheispalveluna rahoitusvälineiden säilyttämistä *(Annettu 29.1.2018, voimaan 1.3.2018)*
- rahastoyhtiöt
- vaihtoehtorahastojen hoitajat, jotka tarjoavat sijoituspalveluja
- ulkomaisten luottolaitosten Suomessa olevat sivuliikkeet
- ulkomaisten maksulaitosten Suomessa olevat sivuliikkeet
- ulkomaisten sijoituspalveluyritysten Suomessa olevat sivuliikkeet
- arvopaperikeskus.

Lisäksi Finanssivalvonta suosittaa, että pörssi noudattaisi luvun 8.3 ohjeita poikkeusoloihin varautumisesta. *(Annettu 29.1.2018, voimaan 1.3.2018)*

1.3 Suhteellisuusperiaate

Näitä määräyksiä ja ohjeita sovelletaan erilaisiin valvottaviin ja erityyppisiin hallintomalleihin. Valvottava voi näitä määräyksiä ja ohjeita soveltaessaan ottaa huomioon toimintansa laadun, laajuuden, monimuotoisuuden ja riskit sekä mahdolliset muut vastaavat arviointiin vaikuttavat seikat, kun se harkitsee, miten se toteuttaa määräykset ja ohjeet tarkoituksenmukaisesti ja tehokkaasti.

1.4 Määritelmät

Valvottavalla tarkoitetaan kaikkia edellä luvussa 1.1 esitettyyn määräysten ja ohjeiden soveltamisalaan kuuluvia Finanssivalvonnasta annetussa laissa tarkoitettuja valvottavia ja ulkomaisia valvottavia.

Operatiivisella riskillä tarkoitetaan tappionvaaraa, joka aiheutuu

- riittämättömistä tai epäonnistuneista sisäisistä prosesseista
- henkilöstöstä
- järjestelmistä
- ulkoisista tekijöistä.

Oikeudelliset riskit sisältyvät operatiivisiin riskeihin. Strategiset riskit on tässä rajattu operatiivisten riskien ulkopuolelle.

Kontrolleilla tarkoitetaan menettelytapoja sen varmistamiseksi, että toiminta saavuttaa tavoitteensa. Kontrolleja ovat kaikki ne toimenpiteet, joiden tarkoituksena on häiriöiden, puutteiden, virheiden ja väärinkäytösten ennaltaehkäisy, havaitseminen ja vähentäminen. Esimerkkejä kontrolleista ovat täsmäytykset, "neljän silmän periaate" sekä vastapuolten vahvistusten vertailu omaan sopimusdokumentaatioon.

Toimivalla johdolla tarkoitetaan valvottavan toimitusjohtajaa sekä kaikkia toimitusjohtajan välittömässä alaisuudessa toimivia henkilöitä, jotka ovat valvottavan ylimmissä johtotehtävissä tai tosiasiallisesti johtavat valvottavan toimintaa.

2 Säädöstausta ja kansainväliset suositukset

2.1 Lainsäädäntö

Näiden määräysten ja ohjeiden aihepiiriin liittyvät seuraavat säädökset:*(Annettu 29.1.2018, voimaan 1.3.2018)*

- luottolaitostoiminnasta annettu laki (610/2014, jäljempänä myös LLL)
- sijoituspalvelulaki (747/2012, jäljempänä myös SipaL)
- sijoitusrahastolaki (48/1999, jäljempänä myös SRL)
- laki vaihtoehtorahastojen hoitajista (162/2014, jäljempänä myös AIFML)
- laki talletuspankkien yhteenliittymästä (599/2010)
- maksulaitoslaki (297/2010, jäljempänä myös MLLlaki rahoitus- ja vakuutusryhmittymien valvonnasta (699/2004)
- laki kaupankäynnistä rahoitusvälineillä (1070/2017, jäljempänä myös RahKL)
- laki arvo-osuusjärjestelmästä ja selvitystoiminnasta (348/2017, jäljempänä myös AOJSL)
- maksupalvelulaki (290/2010)
- valmiuslaki (1552/2011)
- valtioneuvoston päätös huoltovarmuuden tavoitteista (857/2013).

2.2 Euroopan unionin asetukset

Näiden määräysten ja ohjeiden aihepiiriin liittyvät seuraavat Euroopan unionin asetukset:

- Komission delegoitu asetus 2013/231/EU (32013L0231), annettu 19 päivänä joulukuuta 2012 Euroopan parlamentin ja neuvoston direktiivin 2011/61/EU täydentämisestä poikkeuksien, yleisten toimintaedellytysten, säilytysyhteisöjen, vivutuksen, avoimuuden ja valvonnan osalta; *EUVL L 83, 22.3.2013, s. 1-95 (*jatkossa *delegoitu asetus)*
- Euroopan Keskuspankin asetus (EU) N:o 795/2014, annettu 3 päivänä heinäkuuta 2014 systeemisesti merkittäviä maksujärjestelmiä koskevista yleisvalvontavaatimuksista (EKP/2014/28), EUVL L 217, 23.7.2014, s. 16-30

2.3 Euroopan unionin direktiivit

Näiden määräysten ja ohjeiden aihepiiriin liittyvät seuraavat Euroopan unionin direktiivit:*(Annettu 29.1.2018, voimaan 1.3.2018)*

- Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU (32013L0036), annettu 26 päivänä kesäkuuta 2013, oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta; *EUVL L 176, 27.6.2013,s. 338*
- 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*.
- Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366 , annettu 25.11.2015, 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; *EUVL L 337, 23.12.2015.*
- Euroopan parlamentin ja neuvoston direktiivi 2002/87/EY (32002L0087), annettu 16 päivänä joulukuuta 2002, finanssiryhmittymään kuuluvien luottolaitosten, vakuutusyritysten ja sijoituspalveluyritysten lisävalvonnasta sekä neuvoston direktiivien 73/239/ETY, 79/267/ETY, 92/49/ETY, 92/96/ETY, 93/6/ETY ja 93/22/ETY ja Euroopan parlamentin ja neuvoston direktiivien 98/78/EY ja 2000/12/EY muuttamisesta; *EUVL L35, 11.2.2003, s. 1-27.*
- Euroopan yhteisöjen komission direktiivi 2006/73/EY (32006L0073), annettu 10 päivänä elokuuta 2006, Euroopan parlamentin ja neuvoston direktiivin 2004/39/EY täytäntöönpanosta sijoituspalveluyritysten toiminnan järjestämistä koskevien vaatimusten, toiminnan harjoittamisen edellytysten ja kyseisessä direktiivissä määriteltyjen käsitteiden osalta; *EUVL L 241, 2.9.2006, s. 26 – 58*
- Euroopan parlamentin ja neuvoston direktiivi 2009/65/EY (32009L0065), annettu 13 päivänä heinäkuuta 2009, siirtokelpoisiin arvopapereihin kohdistuvaa yhteistä sijoitustoimintaa harjoittavia yrityksiä (yhteissijoitusyritykset) koskevien lakien, asetusten ja hallinnollisten määräysten yhteensovittamisesta, *EUVL L 302, 17.11.2009, s. 32—96*
- Euroopan parlamentin ja neuvoston direktiivi 2011/61/EU (32011L0061), annettu 8.1.2011 vaihtoehtoisten sijoitusrahastojen hoitajista ja direktiivin 2003/41/EY ja 2009/65/EY sekä asetuksen (EY) N:o *1060/2009 ja (EU) N:o 1095/2010 muuttamisesta, EUVL L 174, 1.7.2011, s. 1-73.*

2.4 Finanssivalvonnan määräyksenantovaltuudet

Finanssivalvonnan oikeus antaa määräyksiä perustuu seuraaviin säännöksiin

- Finanssivalvonnasta annetun lain (878/2008) 18 §:n 2 momentti, jonka mukaan Finanssivalvonta voi antaa määräyksiä valvottavan sisäistä valvontaa ja riskienhallintaa koskevien tietojen säännöllisestä toimittamisesta Finanssivalvonnalle

- LLL:n 9 luvun 24 §:n mukaan Finanssivalvonta voi antaa tarkempia määräyksiä 9 luvun 16 §:ssä tarkoitetusta operatiivisesta riskistä
- Talletuspankkien yhteenliittymästä annetun lain 19 §:n 6 momentin mukaan Finanssivalvonta voi antaa tarkempia määräyksiä yhteenliittymään kuuluvien yritysten riskienhallinnasta
- SipaL:n 6 luvun 2 §:n 1 momentista ja SRL:n 6 §:n 5 momentista seuraa, että Finanssivalvonnan LLL:n 9 luvun 24 §:n nojalla antamat määräykset velvoittavat myös mainituissa lainkohdissa tarkoitettuja sijoituspalveluyrityksiä ja rahastoyhtiöitä
- AIFML:n 6 luvun 2 §:n 6 momentin mukaan, joka tarjoaa 3 luvun 2 §:n 2 momentissa ja 3 luvun 3 §:ssä tarkoitettuja palveluja, on aina täytettävä sijoituspalvelulain 6 luvun 2 §:n 1 momentissa säädetyt vaatimukset. SipaL:n 6 luvun 2 §:n 1 momentista seuraa, että Finanssivalvonnan LLL:n 9 luvun 24 §:n nojalla antamat määräykset velvoittavat myös mainituissa lainkohdissa tarkoitettuja vaihtoehtorahastonhoitajia. *(Annettu 29.1.2018, voimaan 1.3.2018)*
- SRL:n 30 a §:n 3 momentin nojalla Finanssivalvonta antaa tarkemmat määräykset rahastoyhtiön riskienhallintajärjestelmille ja muulle sisäiselle valvonnalle asetettavista vaatimuksista
- MLL:n 19 §:n 3 momentin nojalla Finanssivalvonta voi antaa maksupalveludirektiivin täytäntöön panemiseksi tarkempia määräyksiä toiminnan järjestämisestä, sekä sanotun lain 19 a ja 19 b §:ien nojalla operatiivisten ja turvallisuusriskien hallinnasta sekä poikkeamista ja petoksista ilmoittamisesta. Finanssivalvonnan MLL 19 a ja 19 b §:ien nojalla antamat määräykset velvoittavat myös maksupalveluja ilman toimilupaa tarjoavia henkilöitä sekä LLL 9 luvun 16 §:n perusteella maksupalveluja tarjoavia luottolaitoksia. *(Annettu 29.1.2018, voimaan 1.3.2018)*
- Rahoitus- ja vakuutusryhmittymien valvonnasta annetun lain 16 §:n 3 momentin nojalla Finanssivalvonta antaa ryhmittymän emoyritykselle ja omistusyhteisölle tarkempia määräyksiä sisäisen valvonnan ja riskienhallinnan järjestämisestä
- RahKL:n 3 luvun 36§:n 1 momentin 1 kohdan nojalla Finanssivalvonta antaa tarkempia määräyksiä lain 3 luvun 1 §:ssä tarkoitetusta pörssin toiminnan järjestämisestä.

2.5 Kansainväliset suositukset

Näitä määräyksiä ja ohjeita laadittaessa on otettu huomioon seuraavat kansainväliset suositukset:

- Baselin pankkivalvontakomitean suositus *Principles for the Sound Management of Operational Risk* (BIS kesäkuu 2011)
- Euroopan pankkiviranomaisen ohjeistus *Management of Operational Risks in Market-related Activities* (CEBS lokakuu 2010)
- Euroopan pankkiviranomaisen ohjeet sisäisen hallinnon järjestämisestä *Guidelines on Internal Governance* (EBA/GL/2017/11) *(Annettu 29.1.2018, voimaan 1.3.2018)*Baselin pankkivalvontakomitean suositus *High level principles for business continuity* (BIS elokuu 2006)
- Baselin pankkivalvontakomitean suositus *Risk Management Principles for Electronic Banking* (BIS heinäkuu 2003)

- Euroopan arvopaperimarkkinaviranomaisen ohje ”Toiminnan järjestäminen automatisoidussa kaupankäyntiympäristössä: ohjeet kauppapaikkoja, sijoituspalveluyrityksiä ja toimivaltaisia viranomaisia varten” (ESMA helmikuu 2012)
- Baselin komitean “Committee on Payment and Settlement Systems” ja IOSCO:n komitean “Technical Committee” suositus *Principles for financial market infrastructures* (BIS/IOSCO huhtikuu 2012)
- Euroopan pankkiviranomaisen ohjeet internet-maksujen turvallisuudesta *Guidelines on the Security of Internet Payments* (EBA/GL/2014/12_Rev1)
- Euroopan pankkiviranomaisen ohjeet valvonta- ja arviointiprosessin (SREP) yhteydessä tehtävästä ICT-riskien arvioinnista *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)* (EBA/GL/2017/05*) (Annettu 6.11.2017, voimaan 1.3.2018)*
- Euroopan pankkiviranomaisen ohjeet merkittävien häiriöiden raportoinnista *Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)* (EBA/GL/2017/10) *(Annettu 29.1.2018, voimaan 1.3.2018)*
- Euroopan pankkiviranomaisen ohjeet maksupalvelujen operatiivisia riskejä ja turvallisuusriskejä koskevista turvatoimenpiteistä *Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)* (EBA/GL2017/17) *(Annettu 29.1.2018, voimaan 1.3.2018)*
- Euroopan valvontaviranomaisten yhteiskomitean kannanotto *Joint Position on Manufacturers’ Product Oversight and Governance Processes* (marraskuu 2013)

3 Tavoitteet

(1) Näissä määräyksissä ja ohjeissa käsitellään operatiivisten riskien hallinnan periaatteita ja järjestämistä. Lähemmin tarkastellaan prosessien hallintaan, henkilöstöön, tieto- ja maksujärjestelmiin, tietoturvallisuuteen, jatkuvuussuunnitteluun sekä oikeudellisiin riskeihin liittyviä alueita.

(2) Teknologian kehitys, tuotteiden ja palveluiden kehittyminen, uudet riskienhallintamenetelmät, toimintojen ulkoistaminen, yritysjärjestelyt sekä toimintojen kansainvälistyminen ovat monimutkaistaneet toimintaympäristöä ja lisänneet operatiivisia riskejä finanssipalveluiden tuottamisessa.

(3) Maksu- ja selvitysjärjestelmien vakaa toiminta on tärkeää, koska järjestelmissä välitetään ja selvitetään valtaosa taloudessa liikkuvista maksuista. Katkokset ja häiriöt järjestelmissä hankaloittavat asiakkaiden maksuliikennettä ja saattavat siten aiheuttaa laajakantoisia taloudellisia ongelmia.

(4) Näiden määräysten ja ohjeiden tavoitteena on varmistaa seuraavien seikkojen toteutuminen:

- Valvottava järjestää operatiivisten riskien hallinnan toimintansa laajuuden ja laadun asettamien vaatimusten mukaisesti.
- Tarvittaessa riskien hallintaan kuuluvia tehtäviä voidaan ulkoistaa noudattaen toimintojen ulkoistamisesta annettuja Finanssivalvonnan määräyksiä ja ohjeita 1/2012.
- Valvottava huolehtii riittävästä tietohallinnon, tietoturvallisuuden ja toiminnan jatkuvuuden tasosta.
- Finanssivalvonta saa tiedon merkittävistä valvottavan toiminnan häiriöistä ja virheistä ja muista toteutuneista operatiivisen riskin aiheuttamista vahingoista ja tappiotapahtumista.

4 Operatiivisen riskin hallinnan yleiset periaatteet

4.1 Operatiivisen riskin hallinta

(1) Operatiivisen riskin aiheuttama tappio ei ole kaikissa tapauksissa mitattavissa. Riski voi myös toteutua viiveellä ja ilmetä välillisesti esimerkiksi valvottavan maineen ja arvostuksen heikkenemisenä.

(2) Operatiivisen riskin hallinnassa ovat keskeisessä asemassa toimenpiteet havaittujen prosessien ja riskienhallinnan puutteiden ja virheiden korjaamiseksi sekä muut riskien rajoittamistoimet kuten henkilöstöön liittyvät ja tietotekniset varajärjestelyt sekä vakuutusturvan hankkiminen.

(3) Luottolaitostoiminnasta annetussa laissa on säännelty yksityiskohtaisesti operatiivisen riskin hallintaa. LLL:n 9 luvun 16 §:n 1 momentin mukaan luottolaitoksella on oltava menetelmät operatiivisten riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi. Sen on varauduttava ainakin mallintamisriskin sekä harvoin tapahtuvien, vakavien riskitapahtumien toteutumiseen. Luottolaitoksen täytyy selkeästi kuvata, mitä se pitää operatiivisina riskeinä. Sillä on oltava operatiivisen riskin hallintaa koskevat kirjalliset toimintaperiaatteet ja menettelytavat.

4.2 Operatiivisen riskin hallinnan järjestäminen

(4) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuuksien nojalla seuraavan määräyksen riskien hallinnan järjestämisestä.

Määräys (kohdat 5-6)

(5) Valvottavan hallituksen on hyväksyttävä operatiivisen riskin hallinnan periaatteet, jotka kattavat riskin tunnistamisessa, arvioinnissa, seurannassa ja rajoittamisessa käytettävät menetelmät ja prosessit. Periaatteita on määräajoin arvioitava uudelleen niin, että muutokset toimintaympäristössä ja valvottavan omassa liiketoiminnassa otetaan huomioon.

(6) Valvottavan tulee laatia sen omasta liiketoiminnasta johdettu operatiivisen riskin määritelmä, jossa otetaan huomioon valvottavan toiminnan erityispiirteet.

Ohje (kohdat 7-8)

(7) Finanssivalvonta suosittaa, että valvottavan toimiva johto huolehtii operatiivisen riskin hallinnan periaatteiden käytännön toteuttamisesta kaikissa valvottavan toiminnoissa ja konserniin kuuluvissa yhteisöissä. Lisäksi tulisi varmistaa, että työntekijät tunnistavat omaan toimintaansa liittyvät operatiiviset riskit ja niiden hallintaan liittyvät menettelytavat.

(8) Finanssivalvonta suosittaa, että valvottavan hallitus huolehtii, että valvottavan sisäinen tarkastus arvioi säännöllisesti operatiivisen riskin hallinnan tehokkuutta ja kattavuutta.

4.3 Operatiivisten riskien tunnistaminen ja arviointi

(9) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuuksien nojalla seuraavat määräykset riskien hallinnan järjestämisestä.

Määräys (kohdat 10-14)

(10) Valvottavan on tunnistettava kaikkiin merkittäviin tuotteisiinsa, palveluihinsa, toimintoihinsa, prosesseihinsa ja järjestelmiinsä liittyvät operatiiviset riskit, joilla voi olla olennaista vaikutusta asetettujen toiminnan tavoitteiden saavuttamiseen.

(11) Valvottavan on arvioitava uuden tuotteen ja palvelun riskit ennen niiden käyttöönottoa. Arviointi tulee tehdä myös uuden palvelumallin käyttöönoton yhteydessä, jos tuotteita ja palveluita on yhdistelty uudella tavalla, jollei valvottava arvioi, että aikaisemmin tehdyt arviot kattavat uuden palvelumallin käyttöönottoon liittyvät riskit.

(12) Riskien jatkuvassa arvioinnissa on otettava huomioon riskien toteutumisen todennäköisyys ja vaikutukset vahingon sattuessa. Valvottavan on riskinhallinnan suunnittelussaan vahvistettava tarpeelliset riskien vähentämiskeinot ja muut toiminnassa edellytettävät korjaavat toimenpiteet.

(13) Valvottavan on keskeisten toimintojen osalta päätettävä hyväksyttävästä riskinottotasosta ja asetettava merkittäville riskeille limiitit tai muut rajoitteet.

(14) Valvottavan on luotava vaihtoehtoisia toteutumisnäkymiä (skenaarioita), joilla pyritään ottamaan huomioon ainakin keskeisten prosessien, järjestelmien ja henkilöiden toimimattomuus ja ulkoisten tekijöiden vaikutus.

Ohje (kohdat 15-21)

(15) Finanssivalvonta suosittaa, että tärkeimpien tunnistettujen operatiivisten riskien suhteen valvottava ratkaisee, miten riskejä valvotaan, kannetaanko riskit sellaisenaan, pyritäänkö riskejä vähentämään vai vetäydytäänkö kyseisiä operatiivisia riskejä aiheuttavasta liiketoiminnasta.

(16) Finanssivalvonta suosittaa, että riskien arvioinnissa analysoidaan haitallisesti vaikuttavia sisäisiä ja ulkoisia tekijöitä. Sisäisiä tekijöitä ovat esimerkiksi valvottavan juridinen rakenne, organisaatiomuutokset, tarjottavien tuotteiden tai palveluiden monimutkaisuus, henkilöstön ammattitaito ja vaihtuvuus sekä it-järjestelmien tila. Ulkoisia tekijöitä ovat esimerkiksi teknologian kehitys ja toimintojen kansainvälisyys.

(17) Finanssivalvonta suosittaa, että valvottava pyrkii luomaan ennakoivat menettelyt ja mittarit operatiivisen riskin havaitsemiseksi. Sovellettavia menetelmiä voivat olla määrämuotoiset valvottavan organisaation tekemät itsearvioinnit, riskeihin liittyvien vahinkojen tilastointi, toimintaa kuvaavien

kriittisten muuttujien (KRI) käyttö sekä valvottavan omien ja sen vertaisryhmälle sattuneiden vahinkojen läpikäynti.

(18) Finanssivalvonta suosittaa, että valvottava hankkii operatiivisesta riskistä aiheutuvien taloudellisten vaikutusten varalta vakuutusturvaa. Toimivan johdon tehtävänä tulisi olla huolehtia, että vakuutusturvan riittävyyttä ja kustannuksia arvioidaan säännöllisesti ottaen huomioon muutokset valvottavan liiketoiminnassa. Lisäksi tulisi arvioida vakuutussopimuksista aiheutuvia vastapuoliriskejä sekä sopimusyhtiön vakavaraisuutta.

(19) Finanssivalvonta suosittaa, että valvottava ohjeistaa uuden tuotteen ja palvelun hyväksymismenettelyn.

(20) Finanssivalvonta suosittaa, että uuden tuotteen ja palvelun hyväksymismenettely sisältää esimerkiksi seuraavat asiat:

- kuvaus tuotteesta tai palvelusta
- arvio tuotteen tai palvelun sopivuudesta toimintastrategiaan
- maantieteellinen markkina-alue sekä kohderyhmä
- riskikartoitukset (arviot tuotteeseen tai palveluun liittyvistä riskeistä)
- kuvaus sisäisen valvonnan ja riskienhallinnan järjestämisestä uuden tuotteen tai palvelun osalta
- tuotteeseen tai palveluun liittyvien prosessien läpikäynti (esimerkiksi tarjousvaihe, asiakkaan tunnistaminen, myynti, tuotanto, selvitys- ja maksuliikenne)
- oikeudelliset kysymykset ja sopimuksentekovaltuudet
- kuvaus tietojärjestelmistä, tietoturvasta ja palvelun jatkuvuudesta
- ulkoisen ja sisäisen laskennan asettamat vaatimukset
- kuvaus hinnoittelusta, mahdollisista arvostuksista ja hinnoittelumallien käytöstä
- arvio vaikutuksista kannattavuuteen ja vakavaraisuuteen
- arvio vaikutuksista verotukseen
- kuvaus tarvittavasta koulutuksesta ja ohjeistuksesta.

(21) Finanssivalvonta suosittaa, että valvottava esittelee merkittävän uuden tuotteen tai palvelun Finanssivalvonnalle hyvissä ajoin ennen sen käyttöönottoa.

4.4 Operatiivisten riskien seuranta ja vahinkoraportointi

(22) Luvussa 9 on ohjeistettu Finanssivalvonnalle toimitettava ilmoitus toiminnan häiriöistä ja virheistä sekä vuosi-ilmoitus merkittävistä operatiivisen riskin tappiotapahtumista.

(23) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutuksien nojalla seuraavat määräykset riskien hallinnan järjestämisestä.

Määräys (kohdat 24-25)

(24) Valvottavan on säännöllisesti arvioitava havaitsemiensa operatiivisten riskien luonnetta ja riskien toteutumisen todennäköisyyksiä sekä seurattava toteutuneita tappioita ja niiden määrää. Valvottavan on selvitettävä vahinkotapahtumien toteutumiseen vaikuttavat tekijät ja seuraussuhteet.

(25) Valvottavan hallituksen ja toimivan johdon tulee saada tietoa valvottavan eri liiketoiminta-alueiden tärkeimmistä operatiivisista riskeistä. Osana sisäisen valvonnan järjestämistä hallituksen tulee saada säännöllisesti raportit valvottavan tärkeimmistä riskeistä ja vahinkotapahtumista.

Ohje (kohdat 26-29)

(26) Finanssivalvonta suosittaa, että raportoitaviin tietoihin sisällytetään esimerkiksi kuvaus tapahtumasta, siihen johtaneet syyt, arvio suorista ja epäsuorista kustannuksista sekä toimenpiteet vahingon ennaltaehkäisemiseksi. Lisäksi on suositeltavaa raportoida, mihin toimenpiteisiin on vahingon vuoksi ryhdytty sekä korjaavien toimien vastuuhenkilöistä ja aikataulusta.

(27) Finanssivalvonta suosittaa, että valvottavan toimiva johto arvioi säännöllisesti riskienhallinnan menetelmien ja raportointijärjestelmien ajanmukaisuutta, tarkkuutta ja tarkoituksenmukaisuutta. Raportoinnin sisällön laajuutta ja yksityiskohtaisuutta sekä raporttien jakelua ja raportointitiheyttä tulisi arvioida säännöllisesti.

(28) Finanssivalvonta suosittaa, että seurannan ja raportoinnin olennaisuutta varten määritellään rahamääräinen taso, jota suuremmat tapahtumat raportoidaan. Pienistäkin vahingoista ja ns. läheltä piti -tilanteista tulisi raportoida, jos niillä on periaatteellista merkitystä riskienhallinnan toimivuuden kannalta.

(29) Finanssivalvonta suosittaa, että operatiivisen riskin aiheuttamien tappioiden seuranta järjestetään seuraavan taulukon mukaisesti.

Tappiotyyppi	**Esimerkkejä**
Sisäiset väärinkäytökset	kavallus, petos, lahjuksen ottaminen, arvopaperimarkkinarikos tai -rikkomus, vahingonteko, valtuuksien puuttuminen (tai niiden ylittäminen), asiakastietojen väärinkäyttö, tahallinen position väärinraportointi, liikesalaisuuden rikkominen, kiristys
Ulkopuolisen aiheuttamat vahingot	varkaus, ryöstö, petos (esim. maksuvälineellä), väärennös, rahanpesu, murtautuminen tietojärjestelmään, haittaohjelman levittäminen, tietojärjestelmään kohdistuva palvelunestohyökkäys, pommiuhkaus, henkilöstöön kohdistuva uhkailu, kiristys
Työolot, työturvallisuus	työsopimuslain rikkomukset (mm. työaika, työturvallisuus), syrjinnästä aiheutuva korvausvaatimus, palkka-, korvaus- tai irtisanomisriidat, työmarkkinariidat
Menettelytavoista aiheutuvat tappiot	lain ja hyvän tavan vastainen tai harhaanjohtava markkinointi ja palveluntarjonta, luottamuksellisten asiakastietojen väärinkäyttö (esim. markkinointiin), tiedonantovelvollisuuden laiminlyönti asiakkaille, salassapitovelvollisuuden laiminlyönti, selonottovelvollisuuden laiminlyönti, toimeksiantojen säännösten vastainen toteuttaminen, asiakasvarojen säännösten vastainen käsittely, arvopaperimarkkinarikos tai –rikkomus, rahanpesu
Omaisuusvahingot	tulipalo, vesivahinko, tulva

Tietojärjestelmiin liittyvät ongelmat ja keskeytysvahingot	ohjelmistovirhe, tietoliikennehäiriö, käyttökatkos, laiterikko, sähkökatko, ulkoisen palveluntuottajan häiriö
Prosesseihin liittyvät ongelmat	raportointivirhe, virhe asiakastiedoissa, tallennusvirhe tietojärjestelmään, hinnoitteluvirhe, sopimuksen pätemättömyys, puutteellinen dokumentointi, asiakirjan katoaminen, vakuushallinnan puutteet, asiakkaan toimeksiannon epäonnistunut toteutus, ulkoistetun palvelun häiriö, riita ulkopuolisen toimittajan kanssa, kirjanpitovirhe

5 Operatiivisen riskin hallinnan osa-alueita

5.1 Prosessit

(1) Tässä luvussa prosessilla tarkoitetaan tietyn palvelun tai suoritteen tuottamiseksi muodostettua toimintojen ja resurssien kokonaisuutta. Prosessien hallintaan kuuluu asiakastyytyväisyyteen, tehokkuuteen, kannattavuuteen sekä toiminnan luotettavuuteen ja laatuun liittyviä näkökohtia. Prosessien eri vaiheisiin liittyvien operatiivisen riskin kartoittaminen auttaa valvottavaa tunnistamaan ja rajoittamaan operatiivisia riskejä.

(2) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavan määräyksen riskien hallinnan järjestämisestä.

Määräys (kohta 3)

(3) Valvottavan tulee tunnistaa liiketoiminnan kannalta tärkeimmät prosessit. Prosessien eri vaiheisiin on asetettava kontrollit ja niiden riittävyyttä tulee arvioida erityisesti silloin, kun toiminnan laajuus ja sisältö muuttuvat tai prosesseihin tehdään muutoksia.

Ohje (kohdat 4-6)

(4) Finanssivalvonta suosittaa, että valvottava kiinnittää erityistä huomiota prosesseissa eri organisaatioyksiköiden ja yritysten välisiin rajapintoihin, mahdollisiin prosessien epäjatkuvuuskohtiin, maan rajojen yli harjoitettavaan toimintaan sekä maksuliikenteeseen.

(5) Finanssivalvonta suosittaa, että liiketoiminnan kannalta tärkeimmistä prosesseista laaditaan mahdollisimman yhdenmukainen kirjallinen dokumentaatio, jossa kuvataan prosessiin liittyvät tehtävät, vaiheet ja niiden keskinäiset riippuvuudet ja riskikohdat. Lisäksi dokumentaation tulisi koskea tieto- ja materiaalivirtoja, raportointia sekä prosessiin liittyviä sidosryhmiä ja tietojärjestelmiä. Erityisesti tulisi kiinnittää huomiota suurivolyymisen tapahtumakäsittelyn riittävään dokumentointiin ja ohjeistukseen. Prosessikuvaukset tulisi päivittää säännöllisesti.

(6) Finanssivalvonta suosittaa, että valvottavan projektien ja hankkeiden toteutuksessa noudatetaan mahdollisimman yhtenäisiä periaatteita. Tärkeistä projekteista ja hankkeista tulisi laatia riskiarviot etukäteen.

5.2 Oikeudellinen riski

(7) Oikeudellinen riski voi aiheutua ulkoisten tekijöiden, kuten toimintaympäristön muutosten sekä valvottavan oman toiminnan vaikutuksesta. Oikeudellinen riski voi liittyä kaikkeen liiketoimintaan.

Valvottavan toimintaan sovellettavien säädösten ja määräysten tulkintaan, soveltamisalaan sekä voimassaoloon liittyy epävarmuustekijöitä, joista voi aiheutua huomattavia tappioita ja joilla voi olla merkitystä valvottavan oikeudelliseen vastuuseen ja mahdolliseen korvausvelvollisuuteen.

(8) Sopimusten voimassaoloon ja sisältöön liittyvät riitaisuudet voivat vaikuttaa haitallisesti valvottavan toimintaan. Epäedullisista sopimuksista irtautumiseen ja korvaavan sopimuksen solmimiseen voi liittyä tappion vaara. Tämä koskee erityisesti vakioehtoisten sopimusten käyttöä. Myös valvottavan julkistamiin dokumentteihin, kuten esitteisiin ja mainontaan, voi liittyä vahingonkorvauksen mahdollisuus tai maineen ja arvostuksen heikkenemisen riski.

(9) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavan määräyksen riskien hallinnan järjestämisestä.

Määräys (kohta 10)

(10) Valvottavan hallituksen on tunnistettava toimintaan liittyvät merkittävät oikeudelliset riskit sekä varmistettava, että oikeudellisten riskien hallinta on riittävällä tavalla järjestetty.

Ohje (kohdat 11-15)

(11) Finanssivalvonta suosittaa, että valvottavan toimiva johto järjestää oikeudellisten riskien hallinnan ja osoittaa tarvittavat voimavarat riskien tunnistamiseen, seurantaan ja rajoittamiseen eri liiketoiminta-alueilla.

(12) Finanssivalvonta suosittaa, että valvottava varmistaa riittävän asiantuntemuksen oikeudellisen riskin hallitsemiseksi sopimusten ja muiden oikeustoimien solmimista varten. Valvottavan tulisi varmistua, että sopimuskumppanin edustajalla on oikeus allekirjoittaa sopimus.

(13) Finanssivalvonta suosittaa, että valvottava arkistoi sopimuksiin liittyvän aineiston asianmukaisella tavalla ja että sopimusten voimassaoloa sekä niistä mahdollisesti johtuvia tulkintaerimielisyyksiä tai riitoja seurataan.

(14) Finanssivalvonta suosittaa, että valvottava seuraa sekä lainsäädännön että kansainvälisen sääntelyn muutoksia, jolloin se voi ennakolta valmistautua uusien lakien ja määräysten asettamiin vaatimuksiin. Valvottavan tulisi tuntea omaan alaansa liittyvä oikeuskäytäntö.

(15) Finanssivalvonta suosittaa, että rahoitus- ja vakuutusryhmittymän emoyhtiö huolehtii, että ryhmittymään kuuluvilla yhteisöillä on riittävä asiantuntemus molempien sektorien säännöksistä ja määräyksistä. Useissa valtioissa toimintaa harjoittavan valvottavan tulisi ottaa huomioon, että keskeiset oikeusperiaatteet ja oikeuskäytäntö voivat vaihdella huomattavasti eri valtioiden välillä.

5.3 Henkilöstö

(16) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuuksien nojalla seuraavan määräyksen riskien hallinnan järjestämisestä.

Määräys (kohdat 17-20)

(17) Valvottavan tulee varmistaa, että valvottavan palveluksessa työskentelevien ja rekrytoitavien henkilöiden ammattitaito on riittävä suhteutettuna työtehtäviin sekä valvottavan kokoon, toiminnan laajuuteen ja luonteeseen.

(18) Valvottavan tulee järjestää menettelytavat, joilla varmistetaan, että henkilöstö täyttää jatkuvasti ammattitaidolle asetetut vaatimukset kuten muodollisen kelpoisuuden sekä riittävän koulutus- ja kokemustaustan. Uuden työntekijän hyvämaineisuuteen ja taustoihin tulee kiinnittää erityistä huomiota.

(19) Valvottavan toimivan johdon tulee varmistaa, että tehtävien hoitamiseen on varattu riittävästi henkilöstöä. Liiketoiminnan jatkuvuuden turvaamiseksi tulee erityisesti avaintehtäviä hoitavilla henkilöillä olla varahenkilöt palvelusuhteen yllättävän päättymisen tai keskeytymisen varalta.

(20) Valvottavan tulee varmistaa tarpeellisin menettelytavoin, että sen toimihenkilö ei ilmaise asiakkaan tai muun valvottavan toimintaan liittyvän henkilön taloudellista asemaa tai henkilökohtaisia oloja koskevaa seikkaa taikka liike- tai ammattisalaisuutta. Tietojen ilmaiseminen on mahdollista vain laissa säädettyjen edellytysten täyttyessä.

.

6 Tietojärjestelmät ja tietoturvallisuus

6.1 Tietojärjestelmät

(1) LLL:n 9 luvun 16 §:n 2 momentin mukaan luottolaitoksella on oltava riittävät, turvalliset ja toimintavarmat maksu-, arvopaperi- ja muut tietojärjestelmät.

(2) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuuksien nojalla seuraavat määräykset riskien hallinnan järjestämisestä.

Määräys (kohdat 3-6)

(3) Valvottavan hallituksen on varmistettava, että valvottavalla on toiminnan luonteeseen ja laajuuteen nähden riittävät ja asianmukaisesti järjestetyt tietojärjestelmät. Tietojärjestelmien riittävyyttä ja asianmukaisuutta tulee arvioida suhteessa valvottavan oman toiminnan lähtökohtiin, hallituksen asettamiin vaatimuksiin sekä siihen, että järjestelmät tukevat liiketoimintaa hallituksen linjausten mukaisesti.

(4) Valvottavalla tulee olla tarvittava osaaminen, organisaatio ja sisäinen valvonta tiedon tallentamista, siirtämistä, käsittelemistä ja arkistoimista varten. Jos näitä toimintoja ulkoistetaan, tulee valvottavan varmistua siitä, että tietojenkäsittelypalveluja toimittava yritys noudattaa tässä luvussa esitettyjä periaatteita.

(5) Hallituksen on hyväksyttävä valvottavan nykyisten ja arvioitujen tulevien tarpeiden mukainen tietotekniikkastrategia sekä arvioitava sitä määräajoin uudelleen. Lisäksi hallituksen tulee seurata tietotekniikkaan liittyviä kustannuksia.

(6) Järjestelmien tuotantoon siirtoa, muutostenhallintaa ja testausta varten on oltava määrämuotoiset menettelytavat. Järjestelmät on testattava huolellisesti ennen niiden tuotantoon ottoa. Järjestelmille on tehtävä tarvittaessa kuormitus- ja kapasiteettitestaukset.

Ohje (kohdat 7-9)

(7) Finanssivalvonta suosittaa, että valvottava luo toimintamallin, jolla varmistetaan liiketoimintayksiköiden ja tietotekniikkapalveluja tarjoavien yksiköiden yhteistyö. Valvottavan tulisi kuitenkin eriyttää järjestelmäkehitys- ja tuotantotehtävät toisistaan.

(8) Finanssivalvonta suosittaa, että valvottava kehittää järjestelmäkehityksen ja laadunvarmistuksen menetelmät, jotka turvaavat järjestelmien toiminnan suunnitellulla tavalla. Lisäksi järjestelmistä tulisi olla laadittu dokumentaatio, jolla varmistetaan niiden käyttö ja jatkokehittäminen esim. avainhenkilöiden vaihtuessa.

(9) Finanssivalvonta suosittaa, että valvottava kuvaa menettelytavat, joita noudatetaan, kun hankitaan keskeisiä sovelluksia ja laitteita tai solmitaan sopimuksia palvelujen tuottajien kanssa. Valvottavan tulisi varmistaa, että hankinnat ja sopimukset vastaavat valvottavan tarpeita ja toiminnalle asetettuja laatutavoitteita ja että niillä pystytään takaamaan palvelun jatkuvuus.

(10) Finanssivalvonta suosittaa, etta valvottava ottaa tietojärjestelmäriskiensä hallinnassa huomioon Euroopan pankkiviranomaisen ohjeet valvonta- ja arviointiprosessin (SREP) yhteydessä tehtävästä ICT-riskien arvioinnista. *(Annettu 6.11.2017, voimaan 1.3.2018)*

6.2 Tietoturvallisuus

6.2.1 Tietoturvallisuuden määritelmä ja perusvaatimukset

(11) Tietoturvallisuudella tarkoitetaan sitä, että yrityksen tiedot, palvelut, järjestelmät ja tietoliikenne on suojattu ja varmistettu sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä.

(12) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuuksien nojalla seuraavat määräykset tietoturvallisuuden järjestämisestä.

Määräys (kohdat 1-17)

(13) Valvottavan yleisen tietoturvallisuuden tason ja eri tietojärjestelmien turvatasojen on oltava riittävät valvottavan toiminnan luonteeseen ja laajuuteen, tietojärjestelmien uhkien vakavuuteen sekä yleiseen tekniseen kehitystasoon nähden.

(14) Valvottavan hallitus vastaa siitä, että valvottavan tietoturvallisuus on riittävällä tasolla. Tietoturvallisuuden yleisen tason tulee olla hallituksen määrittämä ja hyväksymä. Valvottavan tulee antaa riittävät resurssit sekä määritellä vastuut riittävän tietoturvallisuuden tason ylläpitämiseksi. Valvottavan tulee arvioida tietoturvallisuuden tasoa säännöllisesti. Havaittujen puutteiden korjaamiseksi tulee ryhtyä välittömästi tarvittaviin toimenpiteisiin.

(15) Valvottavan tulee määritellä säilyttämilleen ja käsittelemilleen tiedoille sekä käyttämilleen järjestelmille omistajat, jotka vastaavat tietojen ja järjestelmien käytön periaatteista, käyttövaltuuksista ja turvallisuudesta. Valvottavan tulee luokitella säilyttämänsä ja käsittelemänsä tiedot niiden turvallisuusvaatimusten mukaan sekä laatia käsittelysäännöt eri turvallisuusluokille.

(16) Valvottavan tulee myöntää käyttövaltuudet tietoihin, ohjelmiin ja järjestelmiin sekä valvoa järjestelmien käyttöä johdon hyväksymien yhtenäisten periaatteiden mukaisesti. Käyttövaltuuksien tulee määräytyä käyttäjän työtehtävien perusteella. Valvottavan tulee rajata tietoihin, ohjelmiin ja järjestelmiin pääsy valtuutetuille henkilöille teknisin keinoin. Käyttövaltuuksien loukkaukset tulee selvittää ja ne tulee raportoida organisaatiossa järjestelmistä vastaavalle taholle.

(17) Tietojärjestelmiin pääsyä tulee valvoa. Myös tietojärjestelmissä käsiteltävien tapahtumien kiistämättömyys sekä keskenään kommunikoivien osapuolten tunnistaminen ja todentaminen on hoidettava asianmukaisesti. Lisäksi tietojärjestelmissä käsiteltävät tapahtumat tulee voida jäljittää aukottomasti.

Ohje (kohdat 18-19)

(18) Finanssivalvonta suosittaa, että valvottavat käyttävät hyväksi soveltuvin osin valtionhallinnon tietoturvallisuuden johtoryhmän ohjetta.[1]

(19) Finanssivalvonta suosittaa, että palveluja kehitettäessä varmistetaan, että tapahtumista tehdään asianmukainen lokikirjaus. Lisäksi tulisi ottaa huomioon palveluihin pääsyn valvonta sekä käyttäjien tunnistaminen ja todentaminen.

6.2.2 Tietoturvariskien hallinta ja tietoturvatapausten käsittely

(20) Tietoturvatapauksella tarkoitetaan yrityksen tietoturvaperiaatteiden vastaista tapahtumaa tai tekoa (esimerkiksi virushyökkäystä), tietojärjestelmämurtoa tai tietovuotoa.

(21) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavat määräykset tietoturvariskien hallinnan järjestämisestä.

Määräys (kohdat 22-24)

(22) Tietoturvariskien arviointi tulee liittää osaksi valvottavan riskienhallintaa, jotta voidaan taata, että hallitus ja toimiva johto saavat käsityksen liiketoiminnan kaikkien merkittävien riskien yhteisvaikutuksesta.

(23) Valvottavan tietoturvallisuuden tason arvioinnin tulee perustua tietoturvallisuuteen liittyvien riskien säännönmukaiseen arviointiin. Riskiarvioita tehtäessä tulee määritellä, mitkä ovat valvottavan keskeiset toiminnot ja resurssit, mitä ovat niihin kohdistuvat uhat, kuinka haavoittuvia valvottavan toiminnot ja resurssit ovat näille uhkille sekä miten uhkat toteutuessaan vaikuttavat valvottavan toimintaan. Havaittujen riskien hallitsemiseksi tulee rakentaa riittävät kontrollit. Käyttöönotettavien uusien järjestelmien, tekniikoiden ja palvelujen riskit tulee myös arvioida ennen niiden tuotantoonottoa.

(24) Tietoturvatapaukset on tunnistettava, analysoitava, arkistoitava ja raportoitava organisaatiossa määrätylle vastuutaholle.

6.2.3 Tietoturvallisuutta koskeva ohjeistus ja koulutus

(25) Tietoturvallisuusohjeisiin kuuluvat muun muassa ohjeet käyttövaltuuksien hallinnoinnista, haittaohjelmien torjunnasta sekä internetin ja sähköpostin käytöstä.

(26) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavat määräykset.

Määräys (kohdat 27-28)

(27) Valvottavalla on oltava ajantasaiset hallituksen hyväksymät tietoturvallisuuden periaatteet sekä niitä tukeva tietoturvallisuusohjeistus, joka tulee saattaa valvottavan työntekijöiden tietoon.

(28) Valvottavan tulee määritellä kunkin työntekijän tietoturvallisuusvastuut selkeästi sekä antaa työntekijöille säännöllisesti tietoturvallisuuskoulutusta. Tietoturvallisuuden kehittämisen on oltava jatkuva prosessi ja sille on määriteltävä selkeät esimiesvastuut.

---

[1] *Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010*

6.2.4 Tietoturvallisuuden varmistaminen tietoverkoissa

(29) Verkkopalvelujen turvallisuus koostuu muun muassa palveluissa käytettyjen toimintamallien ja sovellusten sekä teknisten järjestelmien ja tietoliikenneyhteyksien turvallisuudesta.

(30) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavan määräyksen.

Määräys (kohdat 31-32)

(31) Valvottavan tulee arvioida palvelujen sopivuus tietoverkkoon ennen olemassa olevien tai uusien palvelujen käyttöönottoa tietoverkossa. Palveluihin liittyvät keskeiset riskit sekä niiden hallintakeinot tulee dokumentoida ja tarvittavat kontrollit tulee rakentaa riskien hallitsemiseksi. Verkkoliiketoimintaan, tietojärjestelmiin ja sisäisiin toimintaprosesseihin liittyvä sisäinen valvonta ja riskienhallinta tulee suunnitella ja rakentaa niin, että siinä otetaan huomioon organisaation toiminnan luonne ja laajuus sekä toiminnan uhkatekijät.

(32) Valvottavan tulee jatkuvasti arvioida ja kehittää tietojärjestelmiään sekä niiden tietoturvallisuutta sekä suojautua riittävän hyvin erilaisten häiriöiden ja mahdollisten väärinkäytösten varalta.

6.2.5 Tietoturvallisten palveluiden kehittäminen

(33) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavan määräyksen.

Määräys (kohta 34)

(34) Valvottavan tulee arvioida tietoturvariskit kehittäessään uusia palveluita. Tehdyn riskianalyysin perusteella tulee ryhtyä tarvittaviin toimiin riskien hallitsemiseksi.

Ohje (kohta 35)

(35) Finanssivalvonta suosittaa, että valvottava huolehtii riittävän tietoturvallisuuden varmistamiseksi ennen palvelun käyttöönottoa ja palvelua tarjotessaan ainakin seuraavista asioista:

- Järjestelmäkohtaiset tietoturvatestaukset ja -katselmukset on tehty ja järjestelmien turvatason ja mahdollisten häiriöiden jatkuva seuranta ja raportointi on järjestetty. Turvakatselmuksella tarkoitetaan systemaattista järjestelmän, palvelun tai toiminnan turvallisuustason tutkimista sen varmistamiseksi, että tavoitteeksi asetettu turvallisuustaso on saavutettu.
- Palvelun käytettävyyden ja jatkuvuuden varmistamiseksi varajärjestelyt on kuvattu etukäteen ja järjestelmille on tehty toipumissuunnitelmat.
- Järjestelmät on varustettu tarvittavilla virusten ja muiden haittaohjelmien torjuntamekanismeilla.
- Järjestelmät sekä niiden tarvitsemat tietoliikenneyhteydet on suojattu sen varalta, että ne yritetään tukkia esim. palvelunestohyökkäyksillä. Järjestelmät on varustettu pääsynvalvontamekanismeilla ja valvottava on huolehtinut, että käyttövaltuuksien hallinta on järjestetty asianmukaisesti.
- Ulkoinen verkko on erotettu turvajärjestelyillä valvottavan sisäisestä verkosta.

- Järjestelmiä testataan säännöllisin väliajoin ja varsinkin järjestelmämuutosten jälkeen. Havaitut turvallisuuspuutteet korjataan välittömästi.
- Valvottava on varmistanut, että verkkopalvelussa tiedonsiirto ja palveluntarjoajan järjestelmien tiedon käsittely täyttää tiedon luottamuksellisuuden, eheyden ja kiistämättömyyden vaatimukset. Myös keskenään kommunikoivien osapuolten tunnistaminen ja todentaminen tulisi tehdä riittävän luotettavasti.
- Valvottava on varustanut tietojärjestelmät tarkistusmekanismeilla sekä jäljitysketjuilla, joilla turvataan tiedon ja tulosten oikeellisuus ja eheys. Järjestelmissä käsiteltävien tapahtumien tulisi olla aukottomasti jäljitettävissä.
- Järjestelmiin on rakennettu sellaisia kontrolleja, jotka mahdollistavat eri osajärjestelmissä käsiteltyjen tapahtumien täsmäytyksen.
- Palveluita rakennettaessa on otettu huomioon varajärjestelyt, joilla varaudutaan toiminnassa tai järjestelmässä esiintyviin häiriöihin ja katkoihin vaihtoehtoisilla toimintamalleilla tai järjestelmillä. Varajärjestelyjä ovat esimerkiksi tietojenkäsittelyssä ja tietoliikenteessä tarvittavien tärkeiden komponenttien kahdentaminen ja varmuuskopioiden ottaminen.
- Mahdolliset asiakaskohtaiset salasanat on salakirjoitettu järjestelmän sisällä ja välitettäessä niitä järjestelmien välillä.
- Asiakaskohtaisten tunnistautumistietojen (käyttäjätunnukset ja salasanat) luomisessa, käsittelyssä ja asiakkaalle toimittamisessa on noudatettu erityistä varovaisuutta ja vältetty niin sanottuja vaarallisia työyhdistelmiä.
- Järjestelmiin on kerätty lokia sisäänkirjoittautumisista ja niiden yrityksistä sekä palvelun käytöstä. Lokit ja niistä tuotetut raportit käydään säännöllisesti läpi.
- Asiakkaalle annetaan riittävästi tietoa palveluntarjoajasta, tarjotuista palveluista, vastuunjaosta palvelun tarjoajan ja palvelun käyttäjän välillä sekä siitä, miten asiakas voi käyttää palvelua turvallisesti.

7 Maksujärjestelmät ja maksujenvälitys

(1) LLL:n 9 luvun 16 §:n 2 momentin mukaan luottolaitoksella on oltava riittävät, turvalliset ja toimintavarmat maksu-, arvopaperi- ja muut tietojärjestelmät.

(2) MLL 19 a ja 19 b §:iin perustuen maksupalveluja tarjoavalla valvottavalla ja maksupalveluja ilman toimilupaa tarjoavalla henkilöllä on oltava riittävät riskienhallintamenettelyt maksupalvelujen operatiivisten ja turvallisuusriskien hallintaan sekä poikkeamien ja petosten seurantaan ja raportointiin. *(Annettu 29.1.2018, voimaan 1.3.2018)*

(3) Maksujärjestelmällä tarkoitetaan yleensä järjestelmää, jossa

- käytetään sovittuja maksuvälineitä
- osapuolina on luottolaitoksia, maksulaitoksia ja selvitysyhteisöjä
- osapuolet sopivat erilaisista maksujenvälityksen ja riskienhallinnan käytännöistä
- tehdään mahdolliseksi rahan kierto maksajalta saajalle.

(4) Selvitysjärjestelmä toimii maksutapahtumien välittäjänä pankkien välisessä varojen siirrossa ja voi tarjota myös maksutapahtumien katteensiirtoon liittyvää palvelua.

(5) Maksuvälineellä tarkoitetaan maksukorttia, muuta käyttäjäkohtaista välinettä tai menettelytapaa taikka niiden yhdistelmää, jonka käyttämisestä maksutoimeksiantoihin maksupalvelun käyttäjä ja palveluntarjoaja ovat sopineet.

(6) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavat määräykset.

Määräys (kohdat 7-11)

(7) Valvottavan hallituksen tulee hyväksyä maksujenvälityksen periaatteet, jotka koskevat niitä maksu- ja selvitysjärjestelmiä, joihin valvottava osallistuu, sekä maksupalveluita, joita valvottava tarjoaa asiakkailleen. Maksujenvälityksen periaatteiden tulee kattaa nykyinen toiminta ja niissä on otettava huomioon lähivuosien arvioitu kehitys. Hallituksen tulee asettaa tavoitteet toiminnolle tehokkaan, korkealaatuisen ja luotettavan maksujenvälityksen varmistamiseksi ja seuraamiseksi. Myös valvottavan käyttämien selvitysjärjestelmien tulee olla näiden tavoitteiden mukaisia.

(8) Toimiva johto vastaa riittävän osaamisen, voimavarojen ja sisäisen valvonnan järjestämisestä maksujenvälityksen hoitamiseksi tehokkaasti ja turvallisesti. Valvottavan tulee kartoittaa käyttämiinsä maksujenvälitysjärjestelmiin ja maksupalveluihin liittyvät riskit ja päivittää riskikartoitukset säännöllisesti.

(9) Valvottavan maksujenvälitysjärjestelmien tulee olla toimintavarmoja ja turvallisia. Valvottavan tulee huolehtia, että maksujen välityksessä esiintyy mahdollisimman vähän häiriöitä ja viivästyksiä. Pankkien välisen maksuliikenteen hoitamiseksi on oltava riittävät varajärjestelyt.

(10) Maksupalveluja tarjoavalla valvottavalla ja maksupalveluja ilman toimilupaa tarjoavalla henkilöllä tulee olla riittävät riskienhallintamenettelyt tarjoamiinsa maksupalveluihin liittyvien operatiivisten ja turvallisuusriskien hallitsemiseksi. *(Annettu 29.1.2018, voimaan 1.3.2018)*

(11) Maksupalveluja tarjoavan valvottavan ja maksupalveluja ilman toimilupaa tarjoavan henkilön tulee laatia maksupalveluiden operatiivisia ja turvallisuusriskejä koskeva arvio, joka sisältää myös arvion riskienhallintatoimenpiteiden ja valvontamekanismien riittävyydestä. Arvio tulee toimittaa Finanssivalvonnalle vuosittain luvun 9.3 mukaisesti. *(Annettu 29.1.2018, voimaan 1.3.2018)*

Ohje (kohdat 12 -16)

(12) Finanssivalvonta suosittaa, että valvottava toimittaa uusia maksuliikenteeseen kuuluvia palveluita, järjestelmiä ja tekniikoita koskevat riskiarviot Finanssivalvonnalle ennen uusien palvelujen, järjestelmien ja tekniikoiden käyttöönottoa. Riskiarviot tulisi toimittaa Finanssivalvonnalle myös ennen maksuliikenteeseen sekä selvitysjärjestelmiin tehtävien merkittävien muutosten käyttöönottoa.

(13) Finanssivalvonta suosittaa, että valvottava esittelee Finanssivalvonnalle hyvissä ajoin etukäteen uudet maksupalvelunsa sekä olemassa oleviin palveluihin tehtävät merkittävät muutokset ennen niiden käyttöönottoa.

(14) Finanssivalvonta suosittaa, että valvottava ottaa maksupalveluissaan ja niitä kehitettäessä huomioon Euroopan pankkiviranomaisen ohjeet internet-maksujen turvallisuudesta.[2] (*Annettu 21.4.2015, voimaan 1.7.2015).*

(15) Finanssivalvonta suosittaa, etta maksupalveluja tarjoava valvottava ja maksupalveluja ilman toimilupaa tarjoava henkilö noudattaa maksupalvelujen tarjonnassa Euroopan pankkiviranomaisen ohjeita operatiivisten riskien ja turvallisuusriskien hallintaa koskevista turvatoimenpiteistä*. (Annettu 29.1.2018, voimaan 1.3.2018)*

(16) Finanssivalvonta suosittaa, että valvottava, joka osallistuu systeemisesti merkittävän maksu- tai selvitysjärjestelmän toimintaan, noudattaa soveltuvin osin EKP:n asetusta EKP/2014/28, jolla toimeenpannaan CPSS:n ja IOSCO:n antama suositus Principles for financial market infrastructures.

---

[2] Euroopan pankkiviranomaisen internet-maksujen turvallisuutta koskevien ohjeiden (Guidelines on the Security of Internet Payments) suositukset korvataan vaiheittain Euroopan pankkiviranomaisen ohjeilla maksupalveluntarjoajien operatiivisten ja turvallisuusriskien hallinnasta sekä Euroopan komission asetuksella teknisistä sääntelystandardeista koskien asiakkaan vahvaa tunnistamista ja turvallista kommunikointia.

8 Jatkuvuus- ja valmiussuunnittelu

8.1 Säädöstausta

(1) LLL:n 9 luvun 16 §:n 3 momentin mukaan luottolaitoksella on oltava varautumis- ja jatkuvuussuunnitelmat liiketoiminnan vakaviin häiriöihin varautumiseen, toiminnan jatkuvuuden turvaamiseen sekä häiriötilanteissa aiheutuvien vahinkojen rajoittamiseen.

(2) LLL:n 5 luvun 16 §:n mukaan luottolaitoksen tulee varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa osallistumalla rahoitusmarkkinoiden valmiussuunnitteluun ja valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muilla toimilla.

(3) LLL:n 18 luvun 5 §:n mukaan, mitä 5 luvun 17 säädetään varautumisesta, koskee vastaavasti ulkomaisen luottolaitoksen sivuliikettä. Tämä ei koske ulkomaisen ETA-luottolaitoksen sivuliikettä siltä osin kuin sivuliike on luottolaitoksen kotivaltion lainsäädännön nojalla varmistanut tehtäviensä hoitamisen poikkeusoloissa LLL:n 18 luvun 5 §:ää vastaavalla tavalla ja esittänyt siitä Finanssivalvonnalle riittävän selvityksen.

(4) MLL 41 a §:n mukaan maksulaitoksen tulee varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa osallistumalla rahoitusmarkkinoiden valmiussuunnitteluun ja valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muilla toimilla. Ulkomaisen maksulaitoksen sivuliikettä koskee vastaava varautumisvelvollisuus.

(5) SipaL:n 7 luvun 8 §:n mukaan sijoituspalveluyrityksen, joka tarjoaa oheispalveluna rahoitusvälineiden säilyttämistä, tulee varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa osallistumalla rahoitusmarkkinoiden valmiussuunnitteluun ja valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muin toimenpitein. SipaL:n 1 luvun 4 §:n 2 momentin mukaan vaihtoehtorahastojen hoitajaan, joka tarjoaa sijoituspalveluja, sovelletaan valmiussuunnittelua koskevia säännöksiä. (*Annettu 29.1.2018, voimaan 1.3.2018*)

(6) SipaL:n 7 luvun 15 §:n mukaan mitä 8 §:ssä säädetään varautumisesta, koskee vastaavasti ulkomaisen ETA-sijoituspalveluyrityksen sivuliikettä .SipaL:n 1 luvun 7 §:n mukaan kolmannen maan yritykseen, joka tarjoaa sijoituspalvelua tai harjoittaa sijoitustoimintaa Suomessa sivuliikkeen välityksellä, sovelletaan näiden palvelujen osalta, mitä SipaL:n 7 luvun 15 §:ssä säädetään. (*Annettu 29.1.2018, voimaan 1.3.2018*)

(7) SRL:n 4 a §:n mukaan rahastoyhtiön tulee varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa osallistumalla rahoitusmarkkinoiden valmiussuunnitteluun ja valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muin toimenpitein.Vaihtoehtorahastojen hoitajista annetun lain 1 luvun 6 §:n 2 momentin mukaan vaihtoehtorahastojen hoitajiin, jotka vaihtoehtorahastojen hoitajista annetun lain 3 luvun 2 §:n

mukaisesti tarjoavat sijoituspalveluja, sovelletaan SipaL:n 7 luvun 8 §:n mukaista varautumisvelvollisuutta.(*Annettu 29.1.2018, voimaan 1.3.2018*)

(8) AOJSL:n 2 luvun 12 §:n mukaan arvopaperikeskuksen tulee varmistaa arvo-osuusjärjestelmässä olevien tietojen säilyttäminen mahdollisimman häiriöttömästi myös poikkeusoloissa Suomessa olevilla riittävillä tietojärjestelmillä tai muilla keskeytymättömän toiminnan kannalta riittävillä järjestelyillä sekä osallistumalla rahoitusmarkkinoiden valmiussuunnitteluun, valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muilla vastaavilla toimenpiteillä. (*Annettu 29.1.2018, voimaan 1.3.2018*)

8.2 Jatkuvuussuunnittelu

(9) Jatkuvuussuunnittelulla tarkoitetaan varautumista liiketoiminnan keskeytyksiin siten, että valvottava pystyy jatkamaan toimintaansa ja rajoittamaan tappioita erilaisissa liiketoimintaa kohtaavissa häiriötilanteissa. Häiriötilanteita ovat muun muassa valvottavan henkilöstöä, toimitiloja, tietojärjestelmiä tai tietoliikennettä kohdanneet vahingot tai tahalliset teot, vesivahingot, tulipalot sekä katkot esimerkiksi sähkön, lämmön tai veden saannissa. Jatkuvuussuunnittelussa laaditaan tärkeimmille liiketoiminta-alueille jatkuvuussuunnitelmat, joiden pohjalta toimintaa jatketaan mahdollisessa häiriötilanteessa.

(10) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavat määräykset jatkuvuussuunnittelusta.

Määräys (kohdat 11-18)

(11) Valvottavan hallitus vastaa siitä, että valvottavan keskeisillä liiketoiminnoilla on ajantasaiset ja riittävät jatkuvuussuunnitelmat. Toimivan johdon tulee määritellä vastuut valvottavan jatkuvuussuunnittelulle. Valvottavalla tulee olla selkeä toimintamalli jatkuvuussuunnitelmien laatimiseen, ylläpitoon ja testaamiseen sekä jatkuvuussuunnittelun tilanteen seuraamiseen.

(12) Valvottavan tulee kartoittaa ja priorisoida tärkeimmät liiketoimintaprosessinsa. Niille tulee määritellä toipumisajat eli pisin sallittu katko, joka ei vielä häiritse liiketoimintaa. Priorisoiduille prosesseille on suunniteltava vaihtoehtoiset toimintamallit ja toipumismenettelyt toiminnan katkosten varalta. Erityisesti on varmistettava, että liiketoiminnan toipumisen kannalta tärkeät tiedot ovat palautettavissa ajan tasalle.

(13) Tietojärjestelmät ja sovellukset tulee luokitella tärkeysjärjestykseen sen mukaan, kuinka nopeasti niiden on toivuttava erilaisissa häiriötilanteissa. Tietojärjestelmille tulee laatia toipumissuunnitelmat, joissa kuvataan, kuinka eri tietojärjestelmät saadaan toimintakuntoon vakavassa häiriötilanteessa tai katastrofissa.

(14) Varmuuskopiot ja mahdollinen tietojenkäsittelyn varakeskus tulee sijoittaa niin kauas varsinaisesta tietojenkäsittelykeskuksesta, että tiedot ja niiden varmistukset eivät voi tuhoutua samanaikaisesti.

(15) Valvottavan jatkuvuussuunnitelmien tulee pohjautua liiketoimintojen uhka- ja haavoittuvuusanalyyseihin eli selvitykseen tietoihin, järjestelmiin, toimintoihin ja palveluihin kohdistuvista uhkista, haavoittuvuuksista ja riskeistä.

(16) Liiketoiminnan jatkuvuussuunnitelmissa tulee ottaa huomioon toiminnan eri uhkatekijät sekä toimintojen haavoittuvuudet. Jatkuvuussuunnitelmien laajuus tulee suhteuttaa valvottavan toimintojen luonteeseen, laajuuteen ja monimutkaisuuteen. Jatkuvuussuunnitelmien on oltava toimintaa ja tiedottamista ohjaavia erilaisissa häiriötilanteissa.

(17) Valvottavan tulee varautua ulkoisten palveluntarjoajien toiminnan häiriöihin. Jatkuvuussuunnitelmissa on kuvattava, miten ulkoisten palveluntarjoajien toiminnan häiriöiden vaikutuksia valvottavan toimintaan pyritään ehkäisemään ja miten valvottava seuraa ulkoisten palveluntarjoajien jatkuvuussuunnittelua. Sopimuksissa ulkoisten palveluntarjoajien kanssa on edellytettävä, että ulkoiset palveluntarjoajat arvioivat, päivittävät ja testaavat omia järjestelmiään toiminnan häiriöiden varalta.

(18) Jatkuvuussuunnitelmat tulee päivittää säännöllisesti ja ne tulee sopeuttaa valvottavan toiminnan, palvelujen tai strategioiden muuttumiseen. Jatkuvuussuunnitelmia tulee testata ja niiden mukaista toimintaa tulee harjoitella säännöllisesti. Jatkuvuussuunnitelmien ajantasaisuuden ja testauksen seurannalle tulee nimetä vastuuhenkilöt.

8.3 Varautuminen poikkeusoloihin

(19) Poikkeusoloihin varautumiselle asetetut vaatimukset perustuvat valmiuslakiin ja viranomaisten antamaan poikkeusolojen varautumisohjeistukseen. Poikkeusoloilla tarkoitetaan valmiuslain 3 §:ssä määriteltyjä tilanteita. Poikkeusoloihin varautuminen pohjautuu normaaliolojen jatkuvuusjärjestelyihin.

(20) Poikkeusolojen häiriötilanne kestää tyypillisesti pidempään kuin tilanteet, joihin normaaliolojen jatkuvuussuunnitelmassa on varauduttu. Lisäksi poikkeusolojen uhat ovat yleensä vakavampia kuin uhat, joiden varalta jatkuvuussuunnitelmia laaditaan.

(21) Tässä annettuja varautumista koskevia ohjeita voidaan soveltaa myös muihin vakaviin häiriöihin ja kriiseihin kuin valmiuslaissa määriteltyihin poikkeusoloihin. Vakavia häiriöitä ja kriisejä voivat olla esimerkiksi valvottavan henkilöstön toimintakykyä vakavasti vaarantava uhka tai valvottavan toimitilojen tai tietojenkäsittely-ympäristön tuhoutuminen.

(22) Valtioneuvosto on 5.12.2013 antamassaan päätöksessä asettanut yleiset huoltovarmuuden tavoitteet. Rahoitushuoltopoolin vuonna 2009 antamissa varautumisohjeissa asetetaan tarkemmat varautumisen tavoitteet sekä annetaan yksityiskohtaisempia ohjeita poikkeusoloihin varautumisesta.

Ohje (kohdat 24-31)

(24) Finanssivalvonta suosittaa, että valvottava harkitsee riskianalyysin perusteella, pitääkö keskeisten ja tärkeiden palvelujen tuottamisessa käytettävät tuotantojärjestelmät sekä niiden ohjauksen, ylläpidon, järjestelmähallinnan ja teknisen tuen osaaminen säilyttää Suomessa kokonaan tai olennaisilta osin vai riittääkö se, että ne ovat palautettavissa Suomeen ennakkoon suunniteltujen järjestelyjen avulla.

(25) Finanssivalvonta suosittaa, että valvottava huolehtii varajärjestelyistä, joilla turvataan pankkien välinen maksuliikenne, arvopaperien selvitys-, toimitus- ja säilytystoiminta sekä eläkkeiden ja muiden toistuvaissuoritusten maksatukset myös silloin, jos näiden toimintojen

kannalta kriittiset järjestelmät Suomessa tai maan rajojen ulkopuolella eivät ole käytettävissä. Lisäksi valvottavan tulisi varmistaa korttimaksamisen infrastruktuurin ja korttivarmennusten toimivuus Suomessa.

(26) Finanssivalvonta suosittaa, että valvottava varmistaa, että yksittäisen kohteen lamautuminen tai vaurio keskeisten palvelujen tuottamisessa tarvittavissa tieto- ja tietoliikennejärjestelmissä ei lamauta koko järjestelmää. Valvottavan tulisi varajärjestelyin varautua kansainvälisten ja kansallisten tietoliikenneyhteyksien häiriöihin.

(27) Finanssivalvonta suosittaa, että keskeisten palveluiden tuottamisessa tarvittavat tietojärjestelmät ja tietovarastot hajautetaan maantieteellisesti vähintään kahteen riskiprofiililtaan erilaiseen paikkaan. Keskeisiä tietoja ja toimintoja voidaan siirtää Euroopan unionin alueelle edellyttäen, että niiden lainmukaisuus, turvallisuus ja käytettävyys tässä ohjeessa määriteltyjen palvelutavoitteiden toteuttamiseksi on turvattu.

(28) Finanssivalvonta suosittaa, että valvottava varmistaa palveluiden tuottamisessa tarvittavat keskeiset tiedot niin, että varsinaisten tietojenkäsittelykeskusten tai niissä olevien tietojen ja varmistusten tuhoutuessa toiminnan jatkamisen kannalta olennaiset tiedot voidaan palauttaa. Tällaisia perustietoja ovat ainakin asiakkaiden ja asiakassopimusten perustiedot (mm. henkilötiedot) ja asiakkaiden varallisuus- ja velka-asemaa koskevat tiedot. Tietojen palauttaminen erilliseltä varmistukselta yleisesti luettavaan sähköiseen muotoon tulisi testata.

(29) Finanssivalvonta suosittaa, että valvottava ulottaa varautumisen myös ulkoistettuihin toimintoihin siinä laajuudessa kuin poikkeusoloissa ylläpidettävien ydintoimintojen ja -palvelujen turvaaminen edellyttää. Varautumisvaatimukset tulisi ottaa huomioon ulkoistamissopimuksia laadittaessa. Varautumisvelvollisen tulisi arvioida palvelun tarjoajan varautumista ja huolehdittava siitä, että se vastaa asetettuja vaatimuksia. Varautumisvelvollinen tulisi arvioida palvelun tarjoajan varautumista esimerkiksi yhteisillä harjoituksilla tämän kanssa.

(30) Finanssivalvonta suosittaa, että varautumisvelvollinen varmistaa, että sillä on poikkeusoloissa ja vakavissa häiriötilanteissa toimintojen ylläpitämiseen tarvittavat resurssit ja kapasiteetti. Myös henkilöresurssien ja varatoimitilojen saatavuus tulisi suunnitella etukäteen. Resurssien saatavuus tulisi turvata etukäteistoimin niitä tilanteita varten, joissa merkittävä osa henkilöstöä ei ole käytettävissä, osa keskeisiä toimitiloja, laitteita ja järjestelmiä on tuhoutunut tai ei muutoin ole käytettävissä tai toiminta laajalla alueella on estynyt.

(31) Finanssivalvonta suosittaa, että varautumisvelvollinen valvottava hoitaa viranomaisraportoinnin myös poikkeusoloissa.

Valmiussuunnitelma

(32) Valmiussuunnitelmalla tarkoitetaan etukäteen laadittavaa kuvausta toimenpiteistä, joiden avulla varautumisvelvollinen varmistaa toimintansa jatkamisen vakavissa normaaliolojen häiriötilanteissa ja poikkeusoloissa. Valmiussuunnitelma voi olla osana jatkuvuussuunnitelmaa sillä edellytyksellä, että siinä on otettu riittävästi huomioon poikkeusolojen varautumisen tarpeet.

Ohje (kohdat 33-34)

(33) Finanssivalvonta suosittaa, että valvottava ylläpitää ajantasaisen valmiussuunnitelman. Varautumisvelvollisen valvottavan tulisi testata ja harjoitella säännöllisesti valmiussuunnitelman toimivuutta itsenäisesti sekä yhdessä muiden markkinoilla toimivien kanssa.

(34) Finanssivalvonta suosittaa, että valvottava nimeää henkilö tai henkilöt, jotka vastaavat valmiussuunnitelman ylläpidosta ja siitä tiedottamisesta.

9 Raportointi Finanssivalvonnalle

9.1 Ilmoitus toiminnan häiriöistä ja virheistä

(1) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavat määräykset sisäistä valvontaa ja riskienhallintaa koskevien tietojen säännöllisestä toimittamisesta Finanssivalvonnalle. *(Annettu 29.1.2018, voimaan 1.3.2018)*

Määräys (kohdat 2-6)

(2) Valvottavan tulee ilmoittaa Finanssivalvonnalle asiakkaille tarjotuissa palveluissa sekä maksu- ja tietojärjestelmissä esiintyneistä merkittävistä häiriöistä ja virheistä viipymättä niiden ilmaannuttua. Maksujenvälityksessä ja korttimaksamisessa merkittäviksi häiriöiksi katsotaan esimerkiksi suurta määrää asiakkaita koskeva häiriö tai viivästys sekä häiriö, jossa asiakastietoja on joutunut ulkopuoliselle taholle. Finanssivalvonnalle tulee ilmoittaa viipymättä myös sellaiset häiriöt ja virheet, jotka haittaavat tai vaarantavat valvottavan kykyä jatkaa liiketoimintaansa tai vastata velvoitteistaan.

(3) Valvottavan tulee tehdä Finanssivalvonnalle täydentävä ilmoitus häiriön tarkemmista yksityiskohdista mahdollisimman pian ensimmäisen ilmoituksen tekemisen jälkeen.

(4) Ilmoitus tulee tehdä ainakin seuraaviin ryhmiin kuuluvista häiriöistä: *(Annettu 29.1.2018, voimaan 1.3.2018)*

- murtautuminen tietojärjestelmään
- tietoturvaloukkaus
- haittaohjelman levittäminen tietojärjestelmään
- palvelunestohyökkäys.

(5) Ilmoitus tulee tehdä myös seuraavista häiriöistä, jos ne vaikuttavat asiakkaiden saamaan palveluun:

- ohjelmistovirhe
- tietoliikennehäiriö
- käyttökatkos ja laiterikko
- viivästykset maksujenvälityksessä.

(6) Maksupalveluja tarjoavan valvottavan ja maksupalveluja ilman toimilupaa tarjoavan henkilön tulee raportoida merkittävistä maksupalveluita koskevista operatiivisista ja turvallisuutta

koskevista häiriöistä Finanssivalvonnalle noudattaen Euroopan pankkiviranomaisen ohjeita.[3] Raportoinnin tulee kattaa ohjeessa mainitut tiedot ja raportoinnissa tulee noudattaa ohjeen mukaisia merkittävän häiriön luokitteluja ja raportoinnin määräaikoja. *(Annettu 29.1.2018, voimaan 1.3.2018)*

Ohje (kohdat 7-8)

(7) Täydentävä ilmoitus voidaan tehdä Finanssivalvonnan internetsivuilta saatavilla olevalla lomakepohjalla häiriöilmoitus, joka on lähetettävä osoitteeseen hairio@finanssivalvonta.fi. Valvottava voi käyttää myös omaa sisäistä raportointimallia edellyttäen, että se sisältää Finanssivalvonnan lomakepohjalla ilmoitettavat tiedot.

(8) Maksupalveluita koskevista merkittävistä operatiivista ja turvallisuushäiriöistä raportoidaan Euroopan pankkiviranomaisen ohjeiden mukaisesti. Ilmoituslomake on saatavissa Finanssivalvonnan internetsivuilta. Lomake lähetetään osoitteeseen hairio@finanssivalvonta.fi. Kyseisistä häiriöistä ei tarvitse erikseen lähettää kohdan (7) mukaista Finanssivalvonnan häiriöilmoituslomaketta. *(Annettu 29.1.2018, voimaan 1.3.2018)*

9.2 Vuosi-ilmoitus operatiivisen riskin aiheuttamista tappioista

(9) Finanssivalvonnalle toimitettava ilmoitus operatiivisesta riskistä aiheutuneista tappioista tehdään valvottavan sisäisen tappiotietoja koskevan raportoinnin pohjalta. Operatiivisen riskin vahinkotapahtumien raportointi on ohjeistettu luvussa 4.4.

(10) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavan määräyksen sisäistä valvontaa ja riskienhallintaa koskevien tietojen säännöllisestä toimittamisesta Finanssivalvonnalle. *(Annettu 29.1.2018, voimaan 1.3.2018)*

Määräys (kohdat 11 - 14)

(11) Valvottavan tulee tehdä Finanssivalvonnalle edellisenä vuonna havaituista operatiivisen riskin aiheuttamista tappioista vuosi-ilmoitus, joka tulee toimittaa Finanssivalvonnalle 28.2. mennessä.

(12) Vuosi-ilmoitus tulee tehdä kalenterivuoden aikana ilmenneistä euromäärältään viidestä suurimmasta operatiivisen riskin tappiotapahtumasta. Ilmoitusta ei kuitenkaan tarvitse tehdä alle kymmenen tuhannen (10 000) euron vahingoista.

(13) Ilmoituksen tulee sisältää ainakin seuraavat tiedot:

- kuvaus tapahtumasta ja vahingon tyyppi luvun 4.4 luokittelun mukaisesti
- selvitys toimenpiteistä, joihin tapahtuman johdosta on ryhdytty
- selvitys tappion määrästä sekä vakuutuskorvauksista tai muista palautuksista.

(14) Vuosi-ilmoitus on tehtävä käyttäen Finanssivalvonnan internetsivuilta saatavilla olevaa lomakepohjaa vahinkoilmoitus ja lähetettävä osoitteeseen opriskivahinko@finanssivalvonta.fi.

[3] *Euroopan pankkiviranomaisen ohjeet direktiivin (EU)2015/2366 (PSD2) mukaisesta merkittävien häiriöiden raportoinnista.*

Ohje (kohta 15)

(15) Finanssivalvonta suosittaa, että talletuspankkien yhteenliittymän keskusyhteisö toimittaa ilmoituksen yhteenliittymään kuuluvien valvottavien tappioista Finanssivalvonnalle ja että Paikallisosuuspankkiliitto toimittaa ilmoituksen liittoon kuuluvien osuuspankkien tappioista Finanssivalvonnalle.

9.3 Vuosittainen arvio maksupalveluiden operatiivisista ja turvallisuusriskeistä *(Annettu 29.1.2018, voimaan 1.3.2018)*

(16) Finanssivalvonta antaa luvussa 2.4 mainittujen määräyksenantovaltuutusten nojalla seuraavan määräyksen.

Määräys (kohta 17)

(17) Maksupalveluja tarjoavan valvottavan ja maksupalveluja ilman toimilupaa tarjoavan henkilön tulee toimittaa operatiivisia ja turvallisuusriskejä sekä riskienhallintatoimenpiteitä koskeva arvionsa vuosittain Finanssivalvonnalle. Vapaamuotoinen riskiarvio tulee toimittaa 28.2. mennessä osoitteeseen operatiivinenriski@finanssivalvonta.fi. Ensimmäinen arvio tulee toimittaa vuodelta 2018 28.2.2019 mennessä.

10 Kumotut määräykset ja ohjeet

Nämä määräykset ja ohjeet kumoavat voimaan tullessaan seuraavat Finanssivalvonnan standardit:

- Finanssivalvonnan antama standardi 4.4b Operatiivisten riskien hallinta
    - Rahoitustarkastuksen antama standardi RA4.2 Operatiivisiin riskeihin liittyvien tapahtumien ilmoittaminen Rahoitustarkastukselle
    - Finanssivalvonnan antaman standardin 6.1 Maksulaitosten ja maksupalvelua ilman toimilupaa tarjoavien henkilöiden toiminta luku 9.7 Operatiivisten riskien hallinta
    - Finanssivalvonnan antaman standardin RA 6.1 Maksulaitosten ja maksupalvelua ilman toimilupaa tarjoavien henkilöiden toiminta luku 4.3.4 Operatiiviseen riskiin liittyvien tapahtumien ilmoittaminen

11 Muutoshistoria

Näitä määräyksiä ja ohjeita on muutettu sen voimaantulon jälkeen seuraavasti

Annettu 21.4.2015, voimaan 1.7.2015

- korvattu luvuissa 2.5 ja 7 viittaus Euroopan keskuspankin internet-maksamisen turvallisuutta koskeviin ohjeisiin Euroopan pankkiviranomaisen 19.12.2014 julkaisemilla internet-maksujen turvallisuutta koskevilla ohjeilla.

Annettu 6.11.2017, voimaan 1.3.2018

- lisätty lukuun 6.1. viittaus Euroopan pankkiviranomaisen 11.5.2017 julkaisemiin ICT-riskien arviointia koskeviin ohjeisiin, minkä johdosta luvun 6 numerointi on muuttunut.

Annettu 29.1.2018, voimaan 1.3.2018

- muutettu lukuja 1.1. ja 8.1 vastaamaan uuden AOJSL:n säännöksiä.
- muutettu lukuja 2.1, 2.3, 2.4 ja 8.1 vastaamaan uuden RahKL:n säännöksiä.
- muutettu lukua 8.1 vastaamaan muutetun SipaL:n säännöksiä.
- poistettu luvusta 2.4 viittaus SipaL:n 7 luvun 23 §:n 1 momentin 3 kohtaan, sillä Finanssivalvonnan SipaL:n 7 luvun 23 §:n 1 momentin 3 kohtaan sisältynyt määräyksenantovaltuutus on kumottu rahoitusvälineiden markkinat -direktiivi ((EU) 65/2014, MiFID II) kansallisen voimaansaattamisen yhteydessä.
- muutettu lukuja 7 ja 9.1 vastaamaan uudistetun MLL:n säännöksiä, minkä johdosta lukujen numerointi on muuttunut.
- lisätty lukuihin 7 ja 9.1 viittaukset Euroopan pankkiviranomaisen (EBA) julkaisemiin ohjeisiin merkittävien maksupalveluhäiriöiden raportoinnista sekä maksupalveluiden operatiivisten ja turvallisuusriskien hallinnasta, minkä johdosta lukujen numerointi on muuttunut lisätty uusi luku 9.3