



28.10.2014

Julkinen

RVOR, Tuomo Malin

Lausuntoyhteenveto rahoitussektorin operatiivisen riskin hallintaa koskevista määräyksistä ja ohjeista

Kooste lausunnoissa esitetyistä kommentteista	Finanssivalvonnan vastaus
Yleisiä kommentteja Finanssivalvontaa pyydetään varaamaan riittävän pitkä siirtymäaika ohjeistuksen täytäntöönpanolle. (Nordea)	Määräykset ja ohjeet tulevat voimaan 1.2.2015. Raportointi merkittävistä tap- piotapahtumista tehdään ensimmäisen kerran v. 2015 tapahtumista. Lisätään maininta suhteellisuusperiaatteen nou- dattamisesta 1 lukuun.
Luku 1: Soveltamisala ja määritelmät	
Soveltaminen pörssiin tulisi rajata suosituksen luonteise- na vain 6 ja 8 lukuihin. Operatiivisen riskin hallinnan me- netelmiä sekä esim. henkilöriskiä ja oikeudellista riskiä koskevia lukuja (4 ja 5) ei tulisi soveltaa, sillä pörssitoi- minnan riskit eroavat sijoituspalveluyrityksien riskeistä ja asiakkaat ovat ammattimaisia, usein valvottavan ase- massa olevia liikkeenharjoittajia, joihin sovelletaan vaka- varaisuussäännöksiä. (Nasdaq-OMX)	Määräysten ja ohjeiden lukuja 4–6 ja 8 sovelletaan pörssiin, sillä Finanssival- vonnulla on RahKL 2 luvun 44 §:n nojal- la oikeus antaa tarkempia määräyksiä pörssin toiminnan järjestämisestä mu- kaan lukien riskienhallinta. Finanssival- vonnulla tehtävää raportointia koskevaa lukua 9 ei sovelleta pörssiin.
Luku 2: Säädöstausta ja kansainväliset suositukset Luku 3 Tavoitteet	
Suhteellisuusperiaatteen soveltamista koskeva kappale, joka on sijoitettuna tavoitteisiin, tulisi siirtää soveltamis- alan yhteyteen. (Nasdaq-OMX) Tulisi mainita EKP:n asetus 2014/28, jolla toimeenpan- naan CPSS/IOSCO –suositukset systemaattisesti merkittä- vien järjestelmien yleisvalvonnasta. (Suomen Pankki)	Lisätään maininta suhteellisuusperiaat- teen noudattamisesta 1 lukuun. Lisätään viittaus EKP:n asetukseen.
Luku 4 Operatiivisen riskin hallinnan yleiset periaat- teet	
Useissa maissa toimivan valvottavan on tärkeää voida noudattaa yhtenäisiä riskienhallinnan käytänteitä. Yhte- näisten pohjoismaisten viranomaisvaatimusten saavut- tamiseksi Finanssivalvonnan määräyksessä tulisi edellyt- tää, että kansainväliseen konserniin kuuluvan valvotta- van toimiva johto vastaa konsernitasolla päätettyjen toi- mintaperiaatteiden noudattamisesta. Finanssivalvonnan	Finanssivalvonnan määräykset ja ohjeet perustuvat LLL:n ja OYL:n hallintoa kos- keviin säännöksiin. LLL:n 7 luvun 1 §:ssä sekä 9 luvun 3 §:ssä määritellään riskienhallintaan liittyvät hallituksen teh- tävät. Organisaatorakenteeltaan eroavat valvottavat voivat ottaa käyttöön erilaisia



28.10.2014

Julkinen

RVOR, Tuomo Malin

sääntelyn ei tulisi edellyttää tarpeetonta moniportaista päätöksentekoa hallitustasolla. (Nordea) Määräyksissä ja ohjeissa tulisi ottaa kantaa siihen, miten niitä sovelletaan konsernissa noudatettujen päätöksentekomenettelyjen osalta. (Nasdaq-OMX) Kaikille operatiivisille riskeille ei ole mahdollista asettaa limiittejä (kohta 4). (Finanssialan Keskusliitto) Luvun 4.2 kohta 6 tulisi olla määräyksenä, jossa velvoitetaan määrittelemään operatiivinen riski. (Valtiovarainministeriö) Luvun 4.2 kohdassa 8 tulisi olla maininta sisäisen valvonnan raportoinnista hallitukselle. (VM) Kohtaan 11 tulisi lisätä lause ” jollei valvottava arvioi, että aikaisemmin tehdyt arviot kattavat uuden palvelumallin käyttöönottoon liittyvät riskit.” (FK) Kohdassa 12 tulisi mainita ”harvoin tapahtuvat vakavat riskitapahtumat”. (VM) Kohdassa 14 tulisi käyttää termiä toteutumisenäkymät LLL:n 19 luvun 20 §:n terminologiaa vastaavasti. (VM) Kohdassa 16 tulisi käyttää ilmaisua valvottavan juridinen rakenne. (VM) Kohdan 20 suositus hyväksymismenettelyyn kuuluvista asioista tulisi muuttaa esimerkin muotoon. (FK) Käsiteltävistä asioista puuttuvat maantieteellinen markkina-alue ja asiakassegmentti.(VM)	käytännön ratkaisuja päättäessään sisäisestä ohjeistuksesta ja vahvistaessaan muualla samassa konsernissa päätettyä ohjeistusta. Finanssivalvonnan määräykset ja ohjeet perustuvat LLL:n ja OYL:n hallintoa koskeviin säännöksiin. Lisätään maininta suhteellisuusperiaatteen noudattamisesta 1 lukuun. Lisätään ilmaisu ”merkittäville operatiivisille riskeille”. Muutetaan määräykseksi joka täydentää LLL:n 9 luvun 16 §:n vaatimusta. Ei muutosta sillä hallitukselle annettavat raportit kuuluvat sisäisen tarkastuksen normaaleihin tehtäviin. Muutetaan ehdotuksen mukaisesti. Tällaisista riskitapahtumista on maininta luvun 4.1 kohdassa 3. Kohtaa muutetaan ehdotuksen mukaisesti ja ilmaisua selkeytetään. Muutetaan ehdotuksen mukaisesti. Muutetaan ehdotuksen mukaisesti.
Luku 5 Operatiivisen riskin hallinnan osa-alueita	
Luvun 5.1 kohta 1 tulisi muuttaa siten, että riskien ”kartoittaminen” auttaa valvottavaa tunnistamaan riskit. (FK) Kohdan 12 mukaan valvottavan tulisi varmistua vastaapuolen oikeudesta allekirjoittaa sopimus. (FK) Kohdassa 19 tulisi olla maininta, joka mahdollistaa tiedojen luovuttamisen osana työtehtävien hoitamista toiselle	Muutetaan ehdotuksen mukaisesti. Muutetaan ehdotuksen mukaisesti. Ilman erityislakien tekstien referoimista kohdassa viitataan yleisesti salassapito-



28.10.2014

Julkinen

RVOR, Tuomo Malin

vastaavan vaitiolovelvollisuuden piirissä olevalle saman valvottavan työntekijälle. (FK)	velvollisuuteen ja edellytyksiin, joiden vallitessa siitä voidaan poiketa.
Luku 6: Tietojärjestelmät ja tietoturvallisuus	
Luvun 6.1 kohdan 5 mukaan tulisi vaatia, että tietotekniikkastrategiaa arvioidaan määräajoin uudelleen. (VM)	Muutetaan ehdotuksen mukaisesti.
Kohdassa 9 tulisi tarkentaa, että suositus koskee vain keskeisiä sovelluksia. (FK) Kohdassa ei mainita kustannusvaikutuksia. (VM)	Muutetaan ehdotuksen mukaisesti. Kustannusvaikutuksia ei ole tarkoituksenmukaista mainita tässä kohdassa.
Luvun 6.2.1 kohdan 13 mukaan hallituksen on annettava riittävät resurssit tietoturvallisuuden tason ylläpitämiseksi, minkä tulisi olla toimivan johdon tehtävänä. (FK)	Muutetaan ehdotuksen mukaisesti.
Tulisi poistaa luvun 6.2.1 kohdan 15 vaatimus luokitella säilytetty ja käsitelty tieto niiden turvallisuusvaatimusten mukaan sekä laatia käsittelysäännöt eri turvallisuusluokille. Valvottavat ovat jo huomioineet tietoturvapoliitikassaan.(FK)	Ei muutosta sillä tietojen luokittelu ja käsittely turvallisuusvaatimusten mukaan on tietoturvallisuuden perusvaatimuksia.
Kohdan 17 suositus käyttää valtionhallintoa varten laadittuja VAHTI-ohjeita tulisi poistaa. (FK)	Ei muutosta sillä kohta 17 on suositus valvottaville.
Luvun 6.2.4 kohdassa 31 oleva velvollisuus arvioida verkkoliiketoiminnan riskejä säännöllisesti tulisi poistaa. Tietoturvariskien arviointia koskeva vaatimus on riittävä. (FK)	Muutetaan ehdotuksen mukaisesti; kohdan 31 ensimmäinen virke poistetaan.
Luonnoksen mukaan hallituksen tulee tehdä päätökset tietotekniikkastrategiasta (luku 6.1 kohta 5), tietoturvallisuusperiaatteista (luku 6.2.3 kohta 30), maksujenvälityspeeriaatteista (luku 7 kohta 7) sekä määritellä vastuut tietoturvallisuustason ylläpitämiseksi (luku 6.2.1 kohta 13). Vaatimus on esimerkiksi monipolvisesta konsernirakenteesta koostuvien pankkiryhmittymien osalta tarpeeton ja hallinnollisesti raskas. Konserneissa ohjeistus johtaisi siihen, että kunkin konserniyhtiön hallituksen tulisi päättää samoista asioista kuin muissa konserniyhtiössä. (FK)	LLL:n 7 luvun 1 §:ssä sekä 9 luvun 3 §:ssä on määritelty riskienhallintaan liittyvät hallituksen tehtävät. Finanssivalvonnan määräykset ja ohjeet perustuvat LLL:n ja OYL:n hallintoa koskeviin säännöksiin. Lisätään maininta suhteellisuusperiaatteen noudattamisesta 1 lukuun. - Luvun 6.2.1 kohdassa 13 tehtävä poistetaan hallituksen vastuulta.
Luku 7: Maksujärjestelmät ja maksujenvälitys	
Finanssivalvonnan tulisi suosittaa, että merkittävän maksu- ja selvitysjärjestelmän toimintaan osallistuvat valvottavat noudattavat EKP:n asetusta 2014/28, jolla toi-	Lisätään ehdotettu viittaus.



28.10.2014

Julkinen

RVOR, Tuomo Malin

meenpannaan CPSS:n ja IOSCO:n antama suositus "Principles for financial market infrastructure". (SP) Kohdan 12 viittaus EKP:n turvallisuussuosituksiin on tarpeeton. Se tulee korvautumaan maksupalveludirektiivin uudistuksen yhteydessä muulla ohjeistuksella. (FK)	Ei muutosta sillä Finanssivalvonta on sitoutunut muiden valvojen tavoin huomioimaan valvonnassaan nämä suositukset.
Luku 8: Jatkuvuus- ja valmiussuunnittelu	
Palveluntarjoajan toiminnan häiriöihin varautumista koskevaa kohtaa 17 tulisi muokata tai se tulisi poistaa. (FK) Kohdan 21 mukaan varautumista koskevia ohjeita voitaisiin soveltaa myös muihin häiriöihin kuin valmiuslaissa määritelyihin poikkeusoloihin. Ohjeet tulisi rajoittaa normaaliolojen viranomaisvaltuuksien puitteisiin. (FK) Pandemia on mainittu valmiuslaissa. (VM) Kohdassa 22 mainittuja valtioneuvoston huoltovarmuuden tavoitteita ei tulisi vyöryttää toimijoita koskeviksi velvoitteiksi. Ohjeet tulisi antaa vasta rahoitushuoltopoolin antamien ohjeiden valmistuttua. (FK) Kohta 24 tulisi antaa määräyksen muodossa, jolla veloitettaisiin valvottavat huolehtimaan varajärjestelyistä, joilla turvataan mm. pankkien välinen maksuliikenne sekä selvitys-, toimitus- ja säilytystoiminta. (SP) Kohdat 24-30: Finanssivalvonnan tulisi arvioida tarkemmin, onko sen sitovana antamat ohjeistus operatiivisen riskin hallinnasta poikkeusoloja varten riittävän yksityiskohtaista LLL:n 9:16 §:n varautumisvelvollisuuden kannalta. (VM) Kohdat 24 ja 25: yksittäisellä valvottavalla ei ole mahdollisuutta varmistaa mm. koko maksujenvälityksen, korttimaksamisen ja arvopaperikaupan toimivuutta. Valvottavilta ei voi edellyttää omien varajärjestelyjen rakentamista yleisten tietoverkkojen ja Swiftin häiriöiden varalle. Tulisi myös huomioida, että viestintämarkkinalain mukaan teleyrityksille on asetettu velvollisuus varautua poikkeusoloihin. (FK) Kohdassa 25 oleva suositus hajauttaa tietojärjestelmät ja tietovarastot maantieteellisesti ei ole selkeä eikä se ole toteutettavissa esim. terroritekoihin varautumisen osalta. (FK) Kohdan 25 mukaisen keskeisten tietojärjestelmien ja tietovarastojen hajauttamisen tulisi olla mahdollista myös	Kohtaa täsmennetään itse jatkuvuussuunnittelun ja ulkoistussopimuksen sisällön suhteen. Kyseisen johdantokappaleen estämättä valvottavien tulee toimia sovellettavien lakien ja määräysten sekä solmimiensa sopimusten ehtojen mukaisesti. Maininta pandemiasta poistetaan. Ei muutosta sillä valtioneuvoston huoltovarmuuden tavoitteita ei mainita velvoittavana määräyksenä vaan niihin viitataan luvun johdantotekstissä. Finanssivalvonta antaa kohdat ohjeena, sillä tältä osin sillä ei ole määräyksenantovaltuuksia. Valvottavan tulisi mahdollisuuksien mukaan omalta osaltaan sekä osallistumalla keskinäisiin järjestelyihin pyrkiä varautumaan kriittisten järjestelmien toimimattomuuteen. Finanssivalvonta ei anna tarkempia ohjeita, sillä suosituksen noudattaminen riippuu käytännön tilanteista. Finanssivalvonta ei pidä tarkoituksenmukaisena laajentaa suosituksen maan-



28.10.2014

Julkinen

RVOR, Tuomo Malin

EU:n ulkopuolelle, jos asetetut edellytykset muuten täyttyvät. (FK)	tieteellistä ulottuvuutta, vaan harkitsee edellytykset tapauskohtaisesti.
Luku 9: Raportointi Finanssivalvonnalle	
Luku 9.1 kohta 2: maksujenvälitystä koskevan ilmoitusvelvollisuuden tulisi koskea merkittäviä ja laajoja maksuliikehäiriöitä. (FK) Valvottavien tulisi voida käyttää omaa sisäistä raportointimalliaan ilmoittaessaan Finanssivalvonnalle häiriöistä ja virheistä. (FK) Luvun 9.1 ilmoitusmenettelyä ei tulisi soveltaa pörssiin, sillä se sopisi huonosti yhteispohjoismaisiin viranomaisen yhteistoimintakäytänteisiin. Pörssitoiminnan erityispiirteet tulee joka tapauksessa huomioida paremmin. (Nasdaq-OMX)	Tehdään esitetty muutos. Finanssivalvonnan internet-sivuilla olevan häiriöilmoituskaavakkeen käyttö muutetaan suositukseksi. Lukua 9 ei sovelleta pörssiin.