Finanssivalvonnalle

Operatiivisen riskin hallintaa koskeva MOK- luonnos

1. Yleisiä näkökohtia

Luonnoksessa ehdotetaan suosituksia poikkeusoloihin varautumista koskeviin kysymyksiin, joita käsitellään parhaillaan muussa valmisteluprosessissa (huoltovarmuusorganisaatio ja rahoitushuoltopooli) toimialan ja viranomaisten välillä. Ohjeistuksen antaminen tässä yhteydessä vähentää kyseisen valmisteluprosessin merkitystä ja voi johtaa tarpeettomiin epäselvyyksiin ja päällekkäisyyksiin eri viranomaisten normien välillä. Päällekkäisyyksiä poikkeusoloja koskevan valmistelutyön kanssa on kuvattu tarkemmin jäljempänä.

Luonnoksen sisältö on paikoin tarpeettoman yksityiskohtaista, mikä saattaa johtaa ohjeistuksen jatkuvaan tarkistamistarpeeseen toimintojen ja järjestelmien nopeasti muuttuessa. Myös ohjeistuksen riittävä yhdenmukaisuus ainakin muiden pohjoismaiden valvojien normiston kanssa on tärkeää sen varmistamiseksi, että Suomessa toimivat konsernit voivat tarvittavilta osin yhtenäistää sisäiset hallinnolliset prosessit. FK kiinnittää huomiota, että esimerkiksi Ruotsin valvontaviranomaisen ohjeistus on monelta osin ehdotettua luonnosta yleisluonteisempaa.

Luonnoksen lähestymistapa tulisi selkeämmin kohdistua merkittäviin operatiivisiin riskeihin sen sijaan että viitataan kaikkiin osa-alueisiin liittyviin mahdollisiin operatiivisiin riskeihin. Esimerkiksi kappaleen 4.3 kohdan 11 vaatimukseen tulisi lisätä sana ”merkittävät” operatiiviset riskit.

Uuden määräyksen ja ohjeen voimaantulopäiväksi ehdotetaan ajankohtaa 1.9.2014. FK pitää voimaantuloa kohtuuttoman lyhyenä ja ehdottaa sitä myöhennettäväksi neljällä kuukaudella. Tämä antaisi valvottaville mahdollisuuden ottaa käyttöön ohjeistuksen mukaiset toimintamallit. Valvottavien on myös arvioita se, missä nykyiset toimintatavat poikkeavat ohjeistuksessa edellytetystä (GAP analyysi) sekä suunniteltava ja vastuutettava muutosten toteutus.

2. Yksityiskohtaiset kommentit

Finanssivalvonnan määräyksenantovaltuudet (kappale 2.4)

Kappaleen toisessa luetelmakohdassa pitänee lukea ”…Finanssivalvonta voi antaa tarkempia määräyksiä …*operatiivisten riskin hallinnasta*”.

Operatiivisten riskien tunnistaminen ja arviointi (kappale 4.3)

Kohdassa 4 edellytetään limiitin asettamista riskeille, mikä ei monenkaan operatiivisten riskien osalta liene mahdollista.

Ehdotamme kohdan 12 loppuun lisättäväksi seuraavan: *”…, jollei valvottava arvioi, että aikaisemmin tehdyt erilliset arviot kattavat uuden palvelumallin käyttöönottoon liittyvät riskit*.”

Kohdassa 21 määritellään tuotteen ja palvelun hyväksymismenettely yksityiskohtaisilla suosituksilla. Ehdotamme kohdan kirjoittamista esimerkin muotoon tai sisällön muuttamista yleisemmälle tasolle. Näin vältetään erilaisesta kansallisesta sääntelystä seuraava

Finanssialan Keskusliitto
Bulevardi 28, 00120 Helsinki
Puh: 020 793 4200
Faksi: 020 793 4202
etunimi.sukunimi@fkl.fi
www.fkl.fi

Finansbranschens Centralförbund
Bulevarden 28, 00120 Helsingfors, Finland
Tel: +358 20 793 4200
Fax: +358 20 793 4202
fornamn.efternamn@fkl.fi

Federation of Finnish Financial Services
Bulevardi 28, 00120 Helsinki, Finland
Tel: +358 20 793 4200
Fax: +358 20 793 4202
firstname.lastname@fkl.fi

päällekkäinen päätöksenteko monikansallisissa konserneissa, sillä esimerkiksi Ruotsin valvoja on ottanut tältä osin sääntelyyn erilaisen lähestymistavan.

Prosessit (kappale 5.1)

Kohdan 1 mukaan riskien arviointi auttaa valvottavaa tunnistamaan ja rajoittamaan operatiivisia riskejä. Koska operatiivisten riskien hallinnan prosessissa ensin tunnistetaan riskit ja vasta sen jälkeen arvioidaan ne, tulisi kohdassa sekaannusten välttämiseksi todeta esim. että ”*riskien kartoittaminen auttaa*…”.

Oikeudellinen riski (kappale 5.2)

Kohdan 12 suositus siitä, että valvottavalla tulisi olla riittävä tietämys sopimuskumppanissa sovellettavista päätöksentekovaltuuksista, on epätarkoituksenmukainen. Sopimuksen tekemisessä on mahdollista varmistaa, että vastapuolen lukuun toimivalla on oikeus sopimuksen solmimiseen, mutta esim. suuren globaalin yhtiön päätöksentekovaltuuksien tietäminen on käytännössä mahdotonta. Selvityksen tulisi siten rajoittua sen varmistamiseen, että vastapuolen edustajalla on oikeus allekirjoittaa sopimus.

Henkilöstö (kappale 5.3)

Kohta 19 edellyttää, että ”toimihenkilö ei ilman suostumusta ilmaise asiakkaan tai muun valvottavan toimintaa liittyvän henkilön taloudellista asemaa tai henkilökohtaisia oloja koskevaa seikkaa taikka liike- tai ammattisalaisuutta…”. Jotta suostumusta ei tarvittaisi tiedon ilmaisemiseen osana työtehtävien hoitamista esim. työtoverille, tulisi kohtaan tulisi lisätä maininta, joka mahdollistaa tietojen luovuttamisen osana työtehtävien hoitamista toiselle vastaavan vaitiolovelvollisuuden piirissä olevalle työntekijälle.

Tietojärjestelmät (kappale 6.1)

Ehdotamme kohdan 9 sanamuodon täsmentämistä seuraavasti ”Finanssivalvonta suosittaa, että valvottava kuvaa menettelytavat, joita noudatetaan, kun hankintaan tai hyväksytään *keskeisiä* sovelluksia…”.

Tietoturvallisuuden määritelmä ja perusvaatimukset (kappale 6.2.1)

Kohdassa 15 valvottaville asetettaisiin yleinen velvollisuus luokitella säilyttämänsä ja käsittelemänsä tiedot niiden turvallisuusvaatimusten mukaan sekä laatia käsittelysäännöt eri turvallisuusluokille. Tämä vaatimus tulisi poistaa. Ehdotettu määräys ulottuisi kaikkiin valvottavan hallussa tai käsiteltävänä oleviin tietoihin siitä riippumatta, missä muodossa ne ovat, Vaatimuksen toteuttaminen edellyttäisi valvottavilta hyötyihin nähden kohtuuttomia panostuksia. Kyse olisi myös kansallisesta viranomaisvelvoitteesta, mikä hankaloittaisi merkittävästi useissa maissa toimivien valvottavien toimintaa. Käytännössä valvottavat ovat jo nykyisin huomioineet vaatimuksen omissa tietoturvapolitiikoissaan toimintansa edellyttämässä laajuudessa, eli tästäkään syystä FK ei pidä näin kategorisesti muotoiltua velvoitetta perusteltuna.

Emme pidä perusteltuna kohdassa 18 olevaa viittausta valtionhallinnon tietoturvallisuuden johtoryhmän ohjeeseen. VAHTI-ohjeet on laadittu valtionhallinnon sisäiseen käyttöön, eivätkä ne muodosta yhtenäistä, kattavaa tai säännöllisesti ylläpidettävää kokonaisuutta. Paria poikkeusta lukuun ottamatta ohjeet ovat saatavilla vain suomenkielisinä, minkä vuoksi niiden

hyödyntäminen kansainvälisessä liiketoiminta- ja toimittajaympäristössä on käytännössä mahdotonta.

Tietoturvariskien hallinta ja tietoturvatapausten käsittely (kappale 6.2.2)

Kappale 6.2 on kokonaisuudessaan kirjoitettu hyvin yksityiskohtaisesti. Verkkoliiketoiminnan kokonaisriskit tulee kohdan 32 mukaan arvioida säännöllisin väliajoin. Näkemyksemme mukaan ei ole perusteltua edellyttää verkkoliiketoiminnan arviointia muusta liiketoiminnasta poikkeavien edellytyksin niin, että sen riskien säännöllistä arviointia korostetaan. Sen sijaan pidämme perusteltuna säännöstä, jolla edellytetään tietoturvariskien säännöllistä seurantaa ja arviointia.

Hallituksen päätöksenteolle asetetut edellytykset

Luonnoksessa asetetaan hallitukselle velvollisuus

- hyväksyä tietotekniikkastrategia ja seurata tietotekniikkaan liittyviä kustannuksia
- määritellä vastuut riittävän tietoturvallisuuden tason ylläpitämiseksi
- hyväksyä tietoturvallisuusperiaatteet ja sitä tukeva ohjeistus
- hyväksyä maksujenvälityksen periaatteet ja tavoitteiden asettaminen

Kaikissa kohdissa on edellytetty hallituksen päätöstä osa-alueeseen kuuluvissa asioissa. Vaikka luetellut asiat kuuluvat viime kädessä hallituksen vastuulla oleviin seikkoihin, nimenomainen hallitukselle kohdennettu 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 toteaa, että esimerkiksi Ruotsissa toimintaan liittyvä päätöksenteko on osoitettu CEO- tason henkilölle. Useissa maissa toimivissa pankkikonserneissa esim. tietoturvan toiminnallinen ja organisatorinen taso varmistuu tehokkaasti asiaa nimenomaisesti hoitavan tahon toimesta.

Nykyisessä riskienhallintaa koskevassa ohjeessa puhutaan hallituksen sijaan ”ylimmästä johdosta”. Näkemyksemme mukaan ilmaisu ”ylin johto” on toimivampi ja hallinnollisesti perustelu, sillä se mahdollistaa turvallisuustoimintojen vastuuttamisen niitä nimenomaisesti hoitavalle organisaation osalle. Asioissa, joissa päätöksenteko voi olla organisoitu tietylle taholle ilman hallituksen nimenomaista delegointia koskevaa päätöstä, voidaan käyttää ilmaisua ”valvottava” kuten ohjeluonnoksessa onkin huomioitu. Ylipäätään nopeasti muuttuvien ja jatkuvaa päivitystä koskevien yksityiskohtaisten ohjeiden ohjaaminen nimenomaisesti hallitukselle on tehokkuuden ja päätöksenteon kannalta tarpeetonta.

Kappaleen 6.2.1 kohdan 14 mukaan hallituksen on annettava riittävät resurssit tietoturvallisuuden tason ylläpitämiseksi. FK:n näkemyksen mukaan hallituksen tehtäviin kuuluu suuntaviivojen ja tietoturvallisuuden tason asettaminen, mutta resursointi ja vastaavan tyyppiset tehtävät ovat toimivan johdon tehtäviä. Lisäksi on syytä täsmentää, miten yleinen tietoturvallisuuden taso määritellään ja mitataan.

Maksujärjestelmät ja maksujenvälitys (kappale 7)

Kohdan 12 viittaus EKP:n internet-maksamista koskeviin turvallisuussuosituksiin ja niitä koskeviin soveltamisohjeisiin on mielestämme tarpeeton ja itse ohjeistus korvaantuu maksupalveludirektiivin uudistuksen myötä muulla ohjeistuksella.

Jatkuvuussuunnittelu (kappale 8.2)

Kohdan 17 mukaan ”valvojan tulee varautua ulkoisten palveluntarjoajien toiminnan häiriöihin”. Ilmaisu on tulkinnanvarainen. Sitä ei mielestämme tule soveltaa esimerkiksi niin, että valvottavalla tulisi olla oma viestintäinfrastruktuuri ja energiatuotanto sellaisia poikkeustilanteita varten, jotka ovat harvinaisia ja joiden toimittajilla on itsellään varautumisvelvollisuus. Kohtaa on tarpeen jatkovalmistelussa täsmentää tai poistaa kyseinen kohta.

Varautuminen poikkeusoloihin (kappale 8.3)

Kohdassa 21 todetaan, että ohjeessa annettuja varautumista koskevia ohjeita voitaisiin soveltaa myös muihin vakaviin häiriöihin ja kriiseihin kuin valmiuslaissa säädettyihin poikkeusoloihin. Selvyyden vuoksi FK haluaa muistuttaa siitä, että näiden ohjeiden ja niiden soveltamisen täytyy mahtua normaaliolojen viranomaisvaltuuksien ja toimijoiden toimintamahdollisuuksien puitteisiin.

Kohdassa 22 viitataan valtioneuvoston 5.12.2014 antamaan päätökseen huoltovarmuuden tavoitteista (VNp) ikään kuin se olisi rahoitusalan toimijoita sitovaa sääntelyä. FK:n käsityksen mukaan VNp ei koske yksittäisiä toimijoita, vaan se ohjaa valtioneuvoston, ministeriöiden ja niiden alaisten viranomaisten toimintaa. Alan toimijoiden, valtiovarainministeriön, Suomen Pankin, ja Huoltovarmuuskeskuksen välillä käydään parhaillaan keskustelua siitä, miltä osin toimijoiden nykyiset järjestelyt jo ovat riittäviä ja mitä muita toimenpiteitä mahdollisesti tarvittaisiin VNp:ssä kuvattujen tavoitteiden saavuttamiseksi. Tästä syystä FK ei pidä hyvänä sitä, että VNp:ssä viranomaisille asetettuja tavoitteita pyrittäisiin vyöryttämään alan toimijoita sitoviksi velvoitteiksi kopioimalla niitä sellaisinaan Finanssivalvonnan ohjeisiin. FK:n näkemyksen mukaan poikkeusolojen varautumista koskevat määräykset ja ohjeet tulisi antaa vasta sen jälkeen, kun edellä kuvatut keskustelut ja niihin liittyvät selvitykset on saatettu päätökseen.

Kohtien 24 ja 25 osalta FK toteaa, ettei yksittäisellä valvottavalla periaatteessakaan ole mahdollisuutta varmistaa koko maksujenvälityksen, korttimaksamisen, arvopaperikaupan, tms. toimivuutta, vaan valvottavan vastuu rajoittuu omien järjestelmiensä, palvelujensa ja infrastruktuuriensa jatkuvuuden turvaamiseen.

Kohdassa 24 edellytetään rahoitussektorin valvottavien varmistavan korttimaksamisen infrastruktuuri ja korttivarmennusten toimivuuden. Kotimaiseenkin korttimaksamisen tapahtumavälitykseen osallistuvat pankkien lisäksi maksujenvälittäjät, kansainväliset korttiyhtiöt, erilaiset tapahtumaprosessorit sekä kauppiaat globaalisti. FK:n näkemyksen mukaan suositusten toteuttaminen ei ole käytännössä mahdollista rahoitusalan valvottavien toimenpitein, koska se edellyttäisi että rahoitussektorin toimijoilla pitäisi olla varajärjestelyt sen varalta, että niiden sisäiset järjestelmät, pankkien välinen tietoliikenne, kauppiaiden ja varmennuskeskusten tai kauppiaiden ja tapahtumanvälittäjien välinen tietoliikenne on pois käytöstä.

Kohdassa 25 Finanssivalvonta mm. suosittaa, että "Kansainvälisten ja kansallisten tietoliikenneyhteyksien häiriöihin tulisi varautua tietoliikenteen varajärjestelyin, mukaan lukien tilanne, että kansainväliset tietoliikenneyhteydet eivät ole lainkaan käytettävissä.". Näin muotoiltuna suosituksen toteuttamisen voidaan tulkita tarkoittavan, että valvottavien pitäisi rakentaa omat globaalit varajärjestelynsä yleisten tietoverkkojen ja Swiftin mahdollisten häiriöiden varalle. Tämä ei liene mahdollista eikä sellaista vaatimusta pitäisi edes suosituksen tasolla asettaa viranomaisen antamassa määräys ja ohje –dokumentissa. FK muistuttaa myös,

että viestintämarkkinalain 90 §:ssä teleyrityksille asetettu velvollisuus varautua poikkeusoloihin ja normaaliolojen häiriötilanteisiin vastaa sisällöltään täysin rahoitussektorin valvottavien lakiin perustuvaa varautumisvelvoitetta. Tästä syystä FK ei pidä mahdollisena, että tätä velvoitetta voitaisiin laajentaa Finanssivalvonnan määräyksillä tai ohjeilla sellaisiin seikkoihin, jotka ovat valvottavien oman kontrollin ulkopuolella.

Edelleen samassa (25) kohdassa todetaan, että "Keskeisten palveluiden tuottamisessa tarvittavat tietojärjestelmät ja tietovarastot tulisi hajauttaa maantieteellisesti vähintään kahteen riskiprofiililtaan erilaiseen paikkaan." Se, miten vaatimus olisi todellisuudessa toteutettavissa, ei ole selvää. Yksittäisen luonnonkatastrofin, kuten esimerkiksi tulvan, maanjäristyksen tms. osalta vaatimus on vielä toteuttavissa mutta esimerkiksi terroriteko voi käytännössä kohdistua mihin tahansa kohteeseen vaikka sen suojaus olisi kuinka korkealla tasolla. Kahden erilaisen riskiprofiilin laatiminen näihin tilanteisiin on haasteellista ja riskiprofiilistaan erilaisten sijoituspaikkojen toteuttaminen maantieteellisesti rajatulla alueella käytännössä mahdotonta.

Kohdan 25 siirtomahdollisuus on rajattu vain EU:n alueelle. Jatkovalmistelussa tulisi vielä arvioida, voisiko siirtomahdollisuus olla tätä laajempi jos edellytykset muutoin täyttyvät.

Ilmoitus toiminnan häiriöistä ja virheistä (kappale 9.1)

Kohdan 2 mukainen ilmoitusvelvollisuus on maksujenvälityksen osalta tarpeettoman laaja. Muiden palvelujen osalta ilmoitusvelvollisuuden arviointivelvollisuuden olemassaoloa täsmennetään ilmaisulla ”merkittävä”.. Maksuliike on luonteeltaan massaluonteista ja siihen liittyvät tapahtumamäärät ovat suuria. Luonnoksen mukaan yksittäistä asiakasta tai hyvin pientä asiakasjoukkoa koskevat tapahtumat tulisi ilmoittaa, vaikka niiden materiaalinen merkitys olisi vähäinen (esim. jonkun tietokentän puuttuminen varsinaisen varojensiirron toteutuessa normaalisti). Ehdotamme maksuliikehäiriöiden ilmoitusvelvollisuutta koskevaa kohtaa täsmennettäväksi muotoon ”merkittävien tai laajojen”.

FK kiinnittää huomiota siihen, että ilmoitusmenettely ja lomakkeiden sisältö poikkeavat pohjoismaiden välillä. Jotta pankki voisi käyttää konsernin yhdenmukaista prosessia, tulisi sillä olla mahdollisuus käyttää omaa raporttimalliaan edellyttäen että se sisältää viranomaisen vaatimat tiedot.

FINANSSIALAN KESKUSLIITTO

Piia-Noora Kauppi
toimitusjohtaja