EBA/GL/2017/05

11/09/2017

Ohjeet

Ohjeet valvonta- ja arviointiprosessin (SREP) yhteydessä tehtävästä ICT-riskien arvioinnista

1. Noudattamista ja ilmoittamista koskevat velvoitteet

Näiden ohjeiden asema

1. Tämä asiakirja sisältää ohjeita, jotka on annettu asetuksen (EU) N:o 1093/20101 16 artiklan nojalla. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan mukaan toimivaltaisten viranomaisten ja finanssilaitosten on kaikin tavoin pyrittävä noudattamaan ohjeita.

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

Raportointivaatimukset

3. Asetuksen (EU) N:o 1093/2010 16 artiklan 3 kohdan nojalla toimivaltaisten viranomaisten on ilmoitettava Euroopan pankkiviranomaiselle viimeistään 13.11.2017, noudattavatko ne tai aikovatko ne noudattaa näitä ohjeita, sekä syyt niiden noudattamatta jättämiseen. Jos ilmoitusta ei toimiteta tähän määräaikaan mennessä, Euroopan pankkiviranomainen katsoo, etteivät toimivaltaiset viranomaiset noudata ohjeita. Ilmoitukset lähetetään Euroopan pankkiviranomaisen verkkosivustolla olevalla lomakkeella sähköpostitse osoitteeseen compliance@eba.europa.eu. Viitteeksi merkitään ”EBA/GL/2017/05”. Ilmoituksen voi lähettää ainoastaan henkilö, jolla on asianmukaiset valtuudet ilmoittaa ohjeiden tai suositusten noudattamisesta toimivaltaisen viranomaisen puolesta. Myös ohjeiden noudattamisen osalta tehtävistä muutoksista on ilmoitettava Euroopan pankkiviranomaiselle.

4. Ilmoitukset julkaistaan Euroopan pankkiviranomaisen verkkosivustolla 16 artiklan 3 kohdan mukaisesti.

[1] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1093/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan pankkiviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/78/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 12).

2. Sisältö, soveltamisala ja määritelmät

Aihe ja soveltamisala

5. Näiden direktiivin 2013/36/EU[2] 107 artiklan 3 kohdan nojalla laadittujen ohjeiden tavoitteena on yhdenmukaistaa valvontakäytäntöjä, joita noudatetaan direktiivin 2013/36/EU 97 artiklassa tarkoitetun valvonta- ja arviointiprosessin (SREP) yhteydessä tehtävässä tieto- ja viestintäteknologiaa (information and communication technology, ICT) koskevien riskien arvioinnissa. SREP-prosessia täsmennetään valvonta- ja arviointiprosessin yhteisistä menettelyistä ja menetelmistä annetuissa EPV:n ohjeissa[3]. Näissä ohjeissa määritetään erityisesti arviointiperusteet, joita toimivaltaisten viranomaisten tulisi soveltaa, kun ne arvioivat valvontatoimenpiteidensä yhteydessä yhtiöitten ICT-hallintaa ja -strategiaa sekä ICT:n riskialttiutta ja siihen liittyviä valvontajärjestelyjä. Nämä ohjeet ovat olennainen osa EPV:n antamia SREP-ohjeita.

6. Toimivaltaisten viranomaisten tulisi soveltaa näitä ohjeita EPV:n SREP-ohjeissa määritetyllä SREP-soveltamistasolla ja ohjeissa esitettyjen vähimmäis- ja suhteellisuusvaatimusten mukaisesti.

Keitä nämä ohjeet koskevat

7. Ohjeet on tarkoitettu toimivaltaisille viranomaisille, sellaisina kuin ne määritellään asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdan i alakohdassa.

Määritelmät

8. Jollei toisin mainita, direktiivissä 2013/36/EU ja asetuksessa (EU) N:o 575/2013 käytettyjä ja määriteltyjä termejä sekä EPV:n SREP-ohjeiden määritelmiä käytetään näissä ohjeissa samassa merkityksessä. Lisäksi näissä ohjeissa tarkoitetaan

ICT-järjestelmillä	tietyn mekanismin tai verkoston osana olevaa ICT-kokonaisuutta, jolla tuetaan yhtiön toimintoja.
ICT-palveluilla	palveluja, joita ICT-järjestelmät tarjoavat yhdelle tai useammalle yhtiönsisäiselle tai ulkopuoliselle käyttäjälle. Tällaisia palveluja ovat esimerkiksi tiedon syöttö, tallennus ja käsittely sekä raportointipalvelut mutta myös seuranta sekä

[2] Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU, annettu 26 päivänä kesäkuuta 2013, oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta (1) – (EUVL L 176, 27.6.2013).

[3] EBA/GL/2014/13

	liiketoiminnan ja päätöksenteon tukipalvelut.
ICT:n saatavuutta ja jatkuvuutta koskevalla riskillä	riskiä ICT-järjestelmien suorituskykyä ja tietojen saatavuutta haittaavista vaikutuksista, joita ovat muun muassa yhtiön palvelujen nopean palautumisen estyminen ICT-laitteistojen tai ohjelmistojen osissa ilmenevien vikojen jälkeen, ICT-järjestelmän puutteellinen hallinta tai muut haitalliset tapahtumat, joita käsitellään yksityiskohtaisemmin liitteessä.
ICT:n turvallisuusriskillä	riskiä ICT-järjestelmien ja tietojen luvattomasta käytöstä joko yhtiön sisällä tai sen ulkopuolella (esim. kyberhyökkäykset). Riskin yksityiskohtaisempi kuvaus on liitteessä.
ICT:n muutosriskillä	riskiä, joka syntyy yhtiön kyvyttömyydestä toteuttaa ICT-järjestelmän muutokset oikeaan aikaan ja hallitusti erityisesti suurissa ja monimutkaisissa muutosohjelmissa, joita käsitellään yksityiskohtaisemmin liitteessä.
ICT-tiedon eheysriskillä	riskiä siitä, ICT-järjestelmiin tallennetut ja niissä käsitellyt tiedot ovat puutteellisia, virheellisiä tai epäjohdonmukaisia eri ICT-järjestelmissä esimerkiksi siksi, että ICT- kontrollit ovat puutteelliset tai laiminlyöty kokonaan tiedon elinkaaren eri vaiheissa (kuten tietoarkkitehtuurin suunnittelussa, tietomallien ja/tai tietohakemistojen tekemisessä, tiedon syöttämisen tarkastuksissa sekä tiedon poiminnan, -siirron ja -käsittelyn hallinnassa, mukaan lukien saadun tiedon tulkitseminen), mikä heikentää yhtiön valmiutta tarjota palvelujaan ja tuottaa (riskien)hallinta- ja taloustietoja tarkoituksenmukaisella ja oikea-aikaisella tavalla. Riskin yksityiskohtaisempi kuvaus on liitteessä.
ICT:n ulkoistamista koskevalla riskillä	riskiä siitä, että ICT-järjestelmien tai niihin liittyvien palvelujen ulkoistaminen kolmannelle osapuolelle tai jollekin toiselle ryhmän yksikölle (ryhmän sisällä tapahtuva ulkoistaminen) heikentää yhtiön toiminnan tuloksellisuutta ja riskienhallintaa liitteessä yksityiskohtaisemmin selvitettävällä tavalla.

3. Täytäntöönpano

Voimaantulopäivä

9. Näitä ohjeita sovelletaan 1. tammikuuta 2018 alkaen.

4. ICT-riskien arviointia koskevat vaatimukset

1 osasto – Yleiset määräykset

10. Toimivaltaisten viranomaisten tulisi arvioida ICT-riskit, ICT-hallintaa koskevat järjestelyt ja ICT-strategia osana SREP-prosessia ja noudattaa tällöin vähimmäisvaatimuksia ja suhteellisuuskriteerejä, jotka esitetään EPV:n SREP-ohjeiden 2 osastossa. Tämä tarkoittaa erityisesti, että

    a. ICT-riskien arviointitiheys riippuu valvonnan vähimmäisvaatimuksista, jotka määräytyvät sen perusteella, mihin SREP-ohjeiden mukaiseen luokkaan yhtiö asetetaan ja mikä on sen oma valvontaohjelma, ja

    b. ICT-riskien arvioinnin laajuus, yksityiskohtaisuus ja intensiivisyys tulisi suhteuttaa yhtiön kokoon, rakenteeseen ja toimintaympäristöön sekä yhtiön toimintojen luonteeseen, laajuuteen ja monimuotoisuuteen.

11. Suhteellisuusperiaatetta sovelletaan näissä ohjeissa valvonnan ja yhtiön kanssa käytävän vuoropuhelun laajuuteen, tiheyteen ja intensiivisyyteen sekä odotuksiin siitä, mitä vaatimuksia yhtiön tulisi täyttää.

12. Arvioinnin päivittämiseksi toimivaltaiset viranomaiset voivat käyttää tukena ja tarkastella toimia, jotka yhtiö tai toimivaltainen viranomainen on jo toteuttanut muiden riskien arvioinnin yhteydessä, tai SREP-arvioinnin osioita. Suorittaessaan erityisesti näiden ohjeiden mukaisia arviointeja toimivaltaisten viranomaisten tulisi valita valvonta-arvioiden laadintaan tarkoituksenmukaisimmat lähestymistavat ja menetelmät, jotka soveltuvat parhaiten yhtiöön ja ovat oikein suhteutettuja. Arviointitietojen hankkimiseksi toimivaltaisten viranomaisten tulisi hyödyntää jo olemassa ja saatavilla olevaa aineistoa (esim. raportteja ja muita asiakirjoja, yhtiön johdon kanssa pidettyjä (riskienhallinta)kokouksia ja tarkastuskäyntien tuloksia).

13. Toimivaltaisten viranomaisten tulisi laatia yhteenveto näissä ohjeissa esitettyjä kriteerejä koskevien arviointien tuloksista ja hyödyntää niitä laatiakseen päätelmiä SREP-arvioinnin osioista, joita täsmennetään EPV:n SREP-ohjeissa.

14. Näiden ohjeiden 2 osaston mukaisesti suoritetun ICT-hallinnan ja -strategian arvioinnin tulisi johtaa tuloksiin, joita voidaan hyödyntää varsinkin EPV:n SREP-ohjeiden 5 osastossa esitetyssä sisäistä hallintoa ja yhtiön laajuisia kontrollitekijöitä koskevien arviointihavaintojen yhteenvedossa ja ottaa huomioon kyseisen SREP-osion pisteytyksessä. Toimivaltaisten viranomaisten tulisi myös ottaa huomioon, että EPV:n SREP-ohjeiden 4 osaston mukaisesti suoritettuun liiketoimintamallin analyysiin tulisi sisällyttää kaikki ICT-strategian arvioinnin merkittävät haittavaikutukset yhtiön liiketoimintastrategiaan tai kaikki

epäilyt siitä, ettei yhtiöllä ole ehkä riittävästi ICT-resursseja ja ICT-valmiuksia tehdä ja tukea suunniteltuja tärkeitä strategisia muutoksia.

15. Näiden ohjeiden 3 osastossa esitetyn ICT-riskien arvioinnin tulokset tulisi ottaa huomioon operatiivisen riskin arvioinnin tuloksissa ja EPV:n SREP-ohjeiden 6.4 jaksossa esitetyssä pisteytyksessä.

16. On hyvä huomioida, että vaikka toimivaltaisten viranomaisten tulisi yleensä arvioida riskien alaluokkia pääluokkien osana (esim. ICT-riskejä operatiivisen riskin osana), ne voivat arvioida joitakin olennaisina pitämiään alaluokkia myös erikseen. Jos toimivaltainen viranomainen pitää ICT-riskejä olennaisina, näissä ohjeissa on pisteytystaulukko (taulukko 1), jota tulisi käyttää, kun ICT-riskeille halutaan antaa erillinen pisteytys alaluokkana. Taulukko perustuu yleiseen menetelmään, jolla pääomaan kohdistuvat riskit pisteytetään EPV:n SREP-ohjeissa.

17. EPV:n SREP-ohjeiden 6.1 jaksossa esitettyjen kriteerien avulla toimivaltaiset viranomaiset voivat muodostaa käsityksen siitä, tulisiko ICT-riskejä pitää olennaisina ja pitäisikö ne näin ollen arvioida ja pisteyttää operatiivisen riskin yksittäisenä alaluokkana.

18. Soveltaessaan näitä ohjeita toimivaltaisten viranomaisten tulisi tarkastella tarvittaessa liitteessä olevaa esimerkinomaista luetteloa ICT-riskien alaluokista ja riskiskenaarioista. Tällöin tulisi ottaa kuitenkin huomioon, että liitteessä esitetään pääasiallisesti ICT-riskejä, jotka saattavat johtaa mittaviin tappioihin. Toimivaltaiset viranomaiset voivat jättää joitakin taulukkoon sisältyviä ICT-riskejä pois, jos ne eivät ole arvioinnin kannalta merkityksellisiä. Yhtiöiden odotetaan pitävän omaa riskiluokitteluaan eikä käyttävän liitteessä esitettyjä ICT-riskien luokittelua.

19. Kun näitä ohjeita sovelletaan valtioiden rajat ylittävää toimintaa harjoittaviin pankkiryhmiin ja niihin kuuluviin yksiköihin ja on perustettu valvontakollegio, siihen osallistuvien toimivaltaisten viranomaisten tulisi EPV:n SREP-ohjeiden 11.1 jakson mukaisesti tekemänsä SREP-arviointiyhteistyön yhteydessä koordinoida mahdollisimman hyvin toimia, joilla kunkin tietoerän tarkka laajuus ja yksityiskohtaisuus määritellään kaikkien ryhmän yksiköiden osalta yhdenmukaisesti.

2 osasto –Yhtiön ICT-hallinnan ja -strategian arviointi

2.1 Yleiset periaatteet

20. Koska tieto- ja viestintäteknologia on yhtiön moitteettoman toiminnan olennainen edellytys, toimivaltaisten viranomaisten tulisi arvioida, kattaako yhtiön hallinnon ja sisäisen valvonnan järjestäminen riittävästi ICT-järjestelmät ja niihin liittyvät riskit, ja käsitelläänkö ja hallitaanko nämä näkökohdat riittävästi ylimmässä hallintoelimessä.

21. Kun toimivaltaiset viranomaiset laativat tällaisen arvion, niiden tulisi käyttää vertailukohtana hyvän sisäisen hallinnon ja riskienvalvontajärjestelyjen vaatimuksia ja standardeja, jotka on esitetty sisäisen hallinnon järjestämisestä annetuissa EPV:n ohjeissa (GL 44)[4] ja sovellettavassa kansainvälisessä ohjeistuksessa, mikäli näitä voidaan soveltaa ICT-järjestelmien ja -riskien erityisluonne huomioon ottaen.

22. Tämän osaston mukainen arviointi ei koske niitä ICT-järjestelmien tai -riskien hallinnan ja kontrollien erityisosia, jotka painottuvat näiden ohjeiden 3 osastossa käsiteltävien erityisten ICT-riskien hallintaan. Tässä osastossa keskitytäänkin seuraaviin osa-alueisiin:

    a. ICT-strategia – onko yhtiöllä riittävän hallittu ICT-strategia, joka on yhdenmukainen yhtiön liiketoimintastrategian kanssa.

    b. Yleinen sisäinen hallinto – ovatko koko yhtiön sisäiset hallintojärjestelyt riittävät suhteessa yhtiön ICT-järjestelmiin.

    c. ICT-riskit yhtiönyhtiön riskienhallintajärjestelmässä – suojaako yhtiön riskienhallinnan ja sisäisen valvonnan järjestelmä riittävästi yhtiön ICT-järjestelmiä.

23. Edellisen kohdan a alakohta tarjoaa tietoa yhtiön hallinnon eri osista, mutta sen tuloksia olisi käytettävä lähinnä EPV:n SREP-ohjeiden 4 osastossa esitetyn liiketoimintamallin arvioinnissa. Edellisen kohdan b ja c alakohdan mukainen arviointi täydentää EPV:n SREP-ohjeiden 5 osastossa käsiteltyjen aiheiden arviointia, ja sen tuloksia tulisi hyödyntää SREP-ohjeiden 5 osaston mukaisesti tehdyssä arvioinnissa.

24. Näiden ohjeiden 2 osaston mukaisen arvioinnin tuloksia tulisi tarvittaessa hyödyntää myös riskien hallinnan ja kontrollien arvioinnissa, jota käsitellään näiden ohjeiden 3 osastossa.

2.2 ICT-strategia

25. Toimivaltaisten viranomaisten tulisi arvioida tämän kohdan mukaisesti, onko laitoksella käytössä ICT-strategia, joka on riittävällä tavalla yhtiön ylimmän hallintoelimen valvonnassa ja yhdenmukainen liiketoimintastrategian kanssa varsinkin siltä osin kuin on kyse yhtiö tieto- ja viestintätekniikan

[4] EPV:n ohjeet sisäisen valvonnan järjestämisestä, GL 44, 27.9.2011.

pitämisestä ajan tasalla ja tärkeiden ja monimutkaisten ICT-muutosten suunnittelusta ja toteutuksista, ja toimiiko ICT-strategia yhtiö liiketoimintamallin tukena.

2.2.1 ICT-strategian laadinta ja riittävyys

26. Toimivaltaisten viranomaisten tulisi arvioida, onko laitoksella käytössä ICT-strategian laadintaa ja kehittämistä varten järjestelmä, joka on oikein suhteutettu yhtiö ICT-toimintojen luonteeseen, laajuuteen ja monimuotoisuuteen. Tätä arviointia suorittaessaan toimivaltaisten viranomaisten tulisi ottaa huomioon seuraavat seikat:

    a. Liiketoiminnan osa-alueen (-alueiden) toimiva johto[5] osallistuu riittävästi yhtiö strategisten ICT-tavoitteiden määrittelyyn, ja ICT-toiminnosta vastaava toimiva johto on puolestaan tietoinen merkittävien liiketoimintastrategioiden ja -aloitteiden kehittelystä, suunnittelusta ja aloituksesta. Näin varmistetaan, että ICT-järjestelmät, ICT-palvelut ja ICT-toiminnot (eli järjestelmien ja palvelujen hallinnasta ja käytöstä vastaavien tahojen toimet) ovat jatkuvasti yhtiö liiketoimintastrategian mukaiset ja että tieto- ja viestintäteknologiaa päivitetään tehokkaasti.

    b. ICT-strategia dokumentoidaan, ja sen tueksi laaditaan konkreettisia täytäntöönpanosuunnitelmia, joihin sisältyy erityisesti tärkeitä välitavoitteita ja resurssisuunnittelua (kuten taloudelliset resurssit ja henkilöstöresurssit). Näin varmistetaan, että suunnitelmat ovat realistisia ja mahdollistavat ICT-strategian toteuttamisen.

    c. Yhtiö päivittää ICT-strategiansa säännöllisesti ja erityisesti liiketoimintastrategian muutosten yhteydessä. Näin tieto- ja viestintäteknologia vastaa jatkuvasti liiketoiminnan keskipitkän ja pitkän aikavälin tavoitteita, suunnitelmia ja toimintoja.

    d. Yhtiö ylin hallintoelin hyväksyy ICT-strategian ja täytäntöönpanosuunnitelmat ja seuraa strategian täytäntöönpanoa.

2.2.2 ICT-strategian täytäntöönpano

27. Jos yhtiön ICT-strategia edellyttää merkittäviä ja monimutkaisia tieto- ja viestintäteknisiä muutoksia tai muutoksia, jotka vaikuttavat olennaisesti yhtiön liiketoimintamalliin, toimivaltaisten viranomaisten tulisi arvioida, onko laitoksella kontrollit, joka on sen koon, ICT-toimintojen ja muutostoimintojen määrän kannalta tarkoituksenmukainen ja tukee yhtiön ICT-strategian tehokasta täytäntöönpanoa. Tätä arviointia suorittaessaan toimivaltaisten viranomaisten tulisi ottaa kontrolleissa huomioon seuraavat seikat:

    a. Järjestelmä pitää sisällään hallinnon prosessit (esim. strategian eteneminen ja sen rahoituksen seuranta ja raportointi) ja hallintoelimet (esim. projektinhallintatoimisto sekä tieto- ja viestintätekniikan ohjausryhmä tai vastaava), joilla tuetaan tehokkaasti ICT-strategian mukaisten ohjelmien toteutusta.

[5] Toimiva johto ja ylin hallintoelin sellaisina kuin ne määritellään 26.6.2013 annetun direktiivin 2013/36/EU 3 artiklan 7 alakohdassa (ylin hallintoelin) ja 3 artiklan 9 alakohdassa (toimiva johto).

b. Järjestelmässä on määritelty ja jaettu ICT-strategian mukaisten ohjelmien toteuttamistehtävät ja -vastuut ja kiinnitetty erityistä huomiota keskeisten toimijoiden kokemukseen tärkeiden ja monimutkaisten tieto- ja viestintäteknisten muutosten organisoinnista, ohjauksesta ja seurannasta sekä muutosten laajemmista vaikutuksista organisaatioon ja henkilöstöön (esim. muutosvastarinnan hallinnasta sekä koulutuksesta ja viestinnästä).

c. Riippumaton valvontatoiminto ja sisäisen tarkastuksen toiminto ovat mukana varmistamassa, että ICT-strategian täytäntöönpanoon liittyvät riskit on tunnistettu, arvioitu ja niitä on tehokkaasti vähennetty ja että ICT-strategian täytäntöönpanossa käytettävä hallintojärjestelmä on tehokas.

d. Järjestelmään sisältyy suunnitteluprosessi ja sen arviointiprosessi, joiden ansiosta voidaan ratkaista joustavasti havaitut merkittävät ongelmat (esim. täytäntöönpanossa ilmenevät ongelmat tai viivästykset) tai reagoida yhtiön ulkopuoliseen kehitykseen (esim. liiketoimintaympäristön merkittäviin muutoksiin ja teknisiin kysymyksiin tai innovaatioihin). Näin strategian täytäntöönpanosuunnitelmaan voidaan tehdä oikea-aikaisia muutoksia.

2.3 Sisäisen hallinnon järjestäminen

28. Toimivaltaisten viranomaisten tulisi arvioida EPV:n SREP-ohjeiden 5 osaston mukaisesti, onko laitoksella asianmukainen, läpinäkyvä tarkoitukseen sopiva yritysrakenne ja onko se ottanut käyttöön asianmukaiset hallintojärjestelyt. Tässä arvioinnissa tulisi tarkastella erityisesti ICT-järjestelmiä, ja sen yhteydessä tulisi arvioida sisäisen hallinnon järjestämisestä annettujen EPV:n ohjeiden mukaisesti, kykeneekö yhtiö osoittamaan, että

    a. sillä on vankka ja läpinäkyvä organisaatiorakenne, jossa on tieto- ja viestintäteknologiaa koskevat selkeät vastuualueet, kuten ylin hallintoelin ja sen toimikunnat, ja tieto- ja viestintätekniikan keskeiset vastuuhenkilöt (esim. tietohallintopäällikkö, operatiivinen johtaja tai vastaava) ovat välillisesti tai suoraan yhteydessä ylimpään hallintoelimeen sen varmistamiseksi, että tieto- ja viestintäteknologiaan liittyvistä tärkeistä tiedoista ja kysymyksistä raportoidaan riittävästi ylimmälle hallintoelimelle käsittelyä ja päätöksentekoa varten;

    b. ylin hallintoelin tuntee tieto- ja viestintäteknologiaan liittyvät riskit ja puuttuu niihin.

29. Lisäksi toimivaltaisten viranomaisten tulisi EPV:n SREP-ohjeiden 5.2 jakson mukaisesti arvioida, tarkastellaanko tieto- ja viestintätekniikan ulkoistamista koskevissa yhtiön toimintaperiaatteissa ja strategiassa tarvittaessa ICT:n ulkoistamisen vaikutusta yhtiön liiketoimintaan ja liiketoimintamalliin.

2.4 ICT-riski yhtiön riskienhallintajärjestelmässä

30. Kun toimivaltaiset viranomaiset arvioivat koko yhtiön laajuista riskienhallintaa ja kontrolleja EPV:n SREP-ohjeiden 5 osaston mukaisesti, niiden tulisi tutkia, turvaako yhtiön riskienhallinnan ja sisäisen valvonnan järjestelmä riittävästi yhtiön ICT-järjestelmät tavalla, joka on oikein suhteutettu yhtiön kokoon ja

toimintaan ja sen ICT-riskiprofiiliin, joka määritellään näiden ohjeiden 3 osastossa. Toimivaltaisten viranomaisten tulisi selvittää erityisesti seuraavat seikat:

a. riskinottohalu ja ICAAP-prosessi kattavat ICT-riskit osana laajempaa operatiivisen riskin luokkaa yleisen riskistrategian määrittelemiseksi ja sisäisen pääoman määrittämiseksi; ja

b. ICT-riskit sisältyvät koko yhtiön kattavaan riskienhallinnan ja sisäisen valvonnan järjestelmään.

31. Toimivaltaisten viranomaisten tulisi ottaa a alakohdassa esitettyjen seikkojen arvioinnissa huomioon sekä odotetut että epäsuotuisat skenaariot, jotka esimerkiksi sisältyvät yhtiökohtaiseen tai valvonnalliseen stressitestiin.

32. Toimivaltaisten viranomaisten tulisi b alakohdassa esitettyjen seikkojen osalta arvioida, kyetäänkö EPV:n SREP-ohjeiden 104 kohdan a ja d alakohdassa sekä 105 kohdan a ja c alakohdassa yksityiskohtaisesti kuvatuilla riippumattomalla valvontatoiminnolla ja sisäisen tarkastuksen toiminnolla asianmukaisesti takaamaan, että ICT-toiminto on riittävän itsenäinen valvonta- ja tarkastustoiminnoista, kun otetaan huomioon yhtiön koko ja ICT-riskiprofiili.

2.5 Yhteenveto havainnoista

33. Tämän arvioinnin tulosten tulisi näkyä EPV:n SREP-ohjeiden 5 osaston mukaan laaditussa arviointihavaintojen yhteenvedossa, ja niiden tulisi olla osa EPV:n SREP-ohjeiden taulukossa 3 esitettyjen näkökohtien mukaisesti annettua pisteytystä.

34. Laadittaessa päätelmiä ICT-strategian arvioinnista tulisi tarkastella seuraavia seikkoja:

a. Jos toimivaltaiset viranomaiset päätyvät katsomaan, ettei yhtiön hallintojärjestelmä ole riittävä yhtiön ICT-strategian laatimiseksi ja toteuttamiseksi 2.2 kohdan mukaisesti, tämä tieto tulisi esittää EPV:n SREP-ohjeiden 5 osaston 87 kohdan a alakohdan mukaisessa yhtiön sisäisen valvonnan arvioinnissa.

b. Jos toimivaltaiset viranomaiset päätyvät katsomaan 2.2 kohdan mukaisesti laadituissa arvioinneissa, että ICT-strategia on liiketoimintastrategian kanssa huomattavassa ristiriidassa, joka voi haitata merkittävästi yhtiön pitkän aikavälin toimintaa ja/tai taloudellisten tavoitteiden saavuttamista, yhtiön toiminnan ja/tai liiketoimintamallin vakautta tai yhtiön liiketoiminta-alueita tai liiketoiminnan osa-alueita, jotka on määritetty merkittävimmiksi EPV:n SREP-ohjeiden 62 kohdan a alakohdassa, tämä tieto tulisi esittää SREP-ohjeiden 4 osaston 70 kohdan b ja c alakohdan mukaisessa liiketoimintamallin arvioinnissa.

c. Jos toimivaltaiset viranomaiset päätyvät katsomaan 2.2 kohdan mukaisissa arvioinneissa, ettei laitoksella ole mahdollisesti riittäviä ICT-resursseja ja ICT-toimeenpanovalmiuksia tehdä ja tukea suunniteltuja tärkeitä strategisia muutoksia, tämä tieto tulisi esittää EPV:n SREP-ohjeiden 4 osaston 70 kohdan b alakohdan mukaisesti suoritetussa liiketoimintamallin analyysissa.

3 osasto – yhtiön ICT-riskien ja niiden kontrollien arviointi

3.1 Yleiset näkökohdat

35. Toimivaltaisten viranomaisten tulisi arvioida, onko yhtiö asianmukaisesti tunnistanut ja arvioinut ICT-riskit ja vähentänyt niitä. Tämän prosessin tulisi olla osa operatiivisen riskin hallintajärjestelmää ja operatiiviseen riskiin sovellettavan lähestymistavan mukainen.

36. Toimivaltaisten viranomaisten tulisi aluksi tunnistaa olennaiset sisäsyntyiset ICT-riskit, joille yhtiö altistuu tai saattaa altistua, ja sen jälkeen arvioida yhtiön ICT-riskien hallintajärjestelmän, menettelyjen ja kontrollien tehokkuus tällaisten riskien vähentämiseksi. Arviointituloksen tulisi näkyä havaintoyhteenvedossa, jota hyödynnetään SREP-ohjeiden mukaisessa operatiivisen riskin pisteytyksessä. Jos ICT-riskiä pidetään olennaisena ja toimivaltaiset viranomaiset haluavat antaa sille erillisen pisteytyksen, niiden tulisi käyttää taulukkoa 1, jossa ICT-riski pisteytetään operatiivisen riskin alariskinä.

37. Kun toimivaltaiset viranomaiset suorittavat tämän osaston mukaisen arvioinnin, niiden tulisi käyttää valvontaan perustuvan arvioinnin painopisteiden määrittämisen perustana kaikkia saatavilla olevia tietolähteitä, jotka esitetään EPV:n SREP-ohjeiden 6 osaston 127 kohdassa ja joita ovat esimerkiksi yhtiön riskienhallinnan toimet, raportointi ja tulokset. Toimivaltaisten viranomaisten tulisi käyttää tämän arvioinnin suorittamiseksi myös muita tietolähteitä, kuten tarvittaessa seuraavia:

    a. ICT-riskin ja sen kontrollien itsearvioinnit (jos tällainen tieto sisältyy ICAAP-tietoihin);
    b. ICT-riskiä koskeva johdon informaatio, joka toimitetaan yhtiön ylimmälle hallintoelimelle ja josta esimerkkinä voidaan mainita säännöllinen ja tapauskohtainen ICT-riskiraportointi (myös operatiivisten tappioiden tietokanta) ja yhtiön riskienhallintatoiminnolta saadut tiedot ICT-riskeille altistumisesta;
    c. tieto- ja viestintäteknologiaan liittyvät sisäisen ja ulkoisen tarkastuksen tulokset, jotka raportoidaan yhtiön tarkastustoimikunnalle.

3.2 Olennaisten ICT-riskien tunnistaminen

38. Toimivaltaisten viranomaisten tulisi tunnistaa seuraavassa esitettävin toimenpitein olennaiset ICT-riskit, joille yhtiö altistuu tai saattaa altistua.

3.2.1 Yhtiön ICT-riskiprofiilin arviointi

39. Arvioidessaan yhtiön ICT-riskiprofiilia toimivaltaisten viranomaisten tulisi tarkastella kaikkia tietoja yhtiön ICT-riskeistä, kuten 37 kohdassa esitettyjä tietoja ja näiden ohjeiden 2 osastossa käsiteltyjä olennaisia puutteita tai heikkouksia, joita on havaittu ICT-organisaatiossa ja yhtiön laajuisissa

kontrolleissa. Viranomaisten tulisi tarkastella tällaisia tietoja tarvittaessa oikeasuhteisella tavalla. Osana arviointia toimivaltaisten viranomaisten tulisi lisäksi tutkia

a. voiko yhtiön ICT-järjestelmien merkittävä häiriö vaikuttaa rahoitusjärjestelmään joko kansallisella tai kansainvälisellä tasolla;
b. voiko laitokseen kohdistua ICT:n turvallisuusriskejä tai ICT:n saatavuutta ja jatkuvuutta koskevia riskejä, jotka johtuvat internetin riippuvuuksista, innovatiivisten ICT-ratkaisujen laajasta käyttöönotosta tai liiketoimintojen muista jakelukanavista ja saattavat lisätä todennäköisyyttä yhtiön joutumisesta kyberhyökkäysten kohteeksi;
c. voiko yhtiö altistua enemmän ICT:n turvallisuusriskeille, ICT:n saatavuutta ja jatkuvuutta koskeville riskeille, ICT-tiedon eheysriskeille tai ICT:n muutosriskeille tieto- ja viestintäteknisten järjestelmiensä (esim. yritysfuusioiden tai -ostojen jälkeisen) monimutkaisuuden tai vanhanaikaisuuden vuoksi;
d. tehdäänkö laitoksessa merkittäviä muutoksia ICT-järjestelmiin ja/tai ICT-toimintoon (esim. yritysfuusioiden, yritysostojen, divestointien tai yhtiön keskeisten ICT-järjestelmien korvaamisen vuoksi), mikä voi horjuttaa ICT-järjestelmien vakautta tai moitteetonta toimintaa ja aiheuttaa olennaisia ICT:n saatavuutta ja jatkuvuutta koskevia riskejä, ICT:n turvallisuusriskejä, ICT:n muutosriskejä tai ICT-tiedon eheysriskejä;
e. onko yhtiö ulkoistanut ryhmän muille yksiköille tai sen ulkopuolelle ICT-palveluja tai ICT-järjestelmiä, jotka saattavat altistaa yhtiön olennaisille ICT:n ulkoistamista koskeville riskeille;
f. toteutetaanko laitoksessa voimakkaita ICT-kustannusten leikkaustoimenpiteitä, jotka voivat johtaa tarpeellisten ICT-investointien ja -resurssien sekä tietoteknisen osaamisen vähenemiseen ja saattavat lisätä altistumista luokitukseen sisältyville kaikentyyppisille ICT-riskeille;
g. voiko tärkeiden ICT-toimintojen tai -datakeskusten sijainti (esim. eri alueilla tai maissa) altistaa yhtiön luonnonkatastrofeille (esim. tulville tai maanjäristyksille), poliittiselle epävakaudelle tai työmarkkinariidoille ja kansalaislevottomuuksille, jotka voivat olennaisesti lisätä ICT:n saatavuutta ja jatkuvuutta koskevia riskejä ja ICT:n turvallisuusriskejä.

3.2.2 Kriittisten ICT-järjestelmien ja -palvelujen arviointi

40. Osana prosessia, jossa tunnistetaan yhtiön vakavaraisuuteen mahdollisesti merkittävästi vaikuttavia ICT-riskejä, toimivaltaisten viranomaisten tulisi arvioida laitoksessa laadittuja asiakirjoja ja muodostaa näkemys siitä, mitkä ICT-järjestelmät ja -palvelut ovat kriittisiä yhtiön olennaisten toimintojen riittävälle toimivuudelle, saatavuudelle, jatkuvuudelle ja turvallisuudelle.

41. Tätä varten toimivaltaisten viranomaisten tulisi arvioida yhtiön käyttämiä menetelmiä ja prosesseja, joilla määritetään kriittiset ICT-järjestelmät ja -palvelut, ja ottaa huomioon, että yhtiö voi pitää joitakin ICT-järjestelmiä ja -palveluja kriittisinä liiketoiminnan jatkuvuuden ja valmiuden sekä turvallisuuden (esim. petosten ennaltaehkäisemisen) ja/tai luottamuksellisuuden (esim. luottamuksellisten tietojen) näkökulmasta. Arviointia suorittaessaan toimivaltaisten viranomaisten tulisi ottaa huomioon, että kriittisten ICT-järjestelmien ja -palvelujen tulisi täyttää ainakin yksi seuraavista edellytyksistä:

a. ne tukevat yhtiön keskeisiä liiketoimintoja ja jakelukanavia (esim. pankkiautomaatteja sekä internet- ja mobiilipankkitoimintoja);

b. ne tukevat olennaisia hallintoprosesseja ja yhtiön tukitoimintoja, kuten riskienhallintaa (esim. riskienhallinnan ja kassanhallinnan järjestelmiä);

c. niihin sovelletaan (mahdollisia) erityisiä lakisääteisiä tai sääntelyvaatimuksia, joilla joillekin järjestelmän kannalta tärkeille palveluille asetetaan saatavuutta, häiriönsietokykyä, luottamuksellisuutta tai turvallisuutta koskevia tiukennettuja vaatimuksia (esim. tietosuojalainsäädäntö tai mahdolliset palautusaikatavoitteet eli enimmäisaika, jossa järjestelmän tai prosessin tulisi palautua häiriötilanteesta, ja palautuspistetavoite eli enimmäisaika, jolta tietojen katoaminen häiriötilanteessa on siedettävissä) (jos tällaisia vaatimuksia on ja mikäli niitä on sovellettava);

d. niillä käsitellään tai tallennetaan luottamuksellisia tai arkaluonteisia tietoja, joiden luvaton käyttö voisi vaikuttaa huomattavasti yhtiön maineeseen, taloudellisiin tuloksiin tai liiketoiminnan vakauteen ja jatkuvuuteen (esim. arkaluonteisia asiakastietoja sisältävät tietokannat); ja/tai

e. ne tarjoavat perustason toimintoja, jotka ovat välttämättömiä yhtiön asianmukaiselle toiminnalle (esim. tietoliikenne- ja liitettävyyspalvelut, ICT- ja kyberturvallisuuspalvelut).

3.2.3 Kriittisiin ICT-järjestelmiin ja -palveluihin kohdistuvien olennaisten ICT-riskien tunnistaminen

42. Toimivaltaisten viranomaisten tulisi ottaa edellä mainitut arvioinnit yhtiön ICT-riskiprofiilista ja kriittisistä ICT-järjestelmistä ja -palveluista huomioon muodostaessaan käsityksen olennaisista ICT-riskeistä, joilla voi olla valvojan laatiman arvioinnin mukaan merkittävä vakavaraisuusvaikutus yhtiön kriittisiin ICT-järjestelmiin ja -palveluihin.

43. Arvioidessaan ICT-riskien mahdollista vaikutusta yhtiön kriittisiin ICT-järjestelmiin ja -palveluihin, toimivaltaisten viranomaisten tulisi tarkastella

a. taloudellista vaikutusta, kuten (vähintään) varojen tai omaisuuserien menetystä, asiakkaille mahdollisesti maksettavia korvauksia, oikeudellisista ja korjaustoimenpiteistä aiheutuvia kustannuksia, sopimusvahinkoja ja menetettyjä tuottoja;

b. liiketoiminnan mahdollisia häiriöitä ottaen (vähintään) huomioon häiriytyneiden rahoituspalvelujen kriittisyyden sekä häiriöistä mahdollisesti kärsineiden asiakkaiden ja/tai sivuliikkeiden ja työntekijöiden lukumäärän;

c. mahdollista vaikutusta yhtiön maineelle häiriöistä kärsineiden pankkipalvelujen tai operatiivisten toimintojen kriittisyyden perusteella (esim. asiakastietojen anastaminen), häiriöistä kärsineiden ICT-järjestelmien ja -palvelujen julkisuuskuvaa/näkyvyyttä (esim. mobiili- ja verkkopankkitoimintojen järjestelmät, myyntipisteet, pankkiautomaatit tai maksujärjestelmät);

d. sääntelyn vaikutusta, kuten sääntelyviranomaisen esittämää julkista arvostelua, viranomaissakkoja tai jopa toimilupiin tehtäviä muutoksia;

e. strategista vaikutusta laitokseen esimerkiksi tilanteessa, jossa strateginen tuote tai liiketoimintasuunnitelma vaarantuu tai anastetaan.

44. Sen jälkeen toimivaltaisten viranomaisten tulisi kartoittaa tunnistetut ICT-riskit, joita pidetään olennaisina, ja jakaa ne seuraaviin ICT-riskiluokkiin, joihin sisältyviä riskejä havainnollistetaan ja kuvataan tarkemmin liitteessä. Toimivaltaisten viranomaisten tulisi tarkastella liitteessä olevia ICT-riskejä osana 3 osaston mukaisesti laadittavaa arviota.

    a. ICT:n saatavuutta ja jatkuvuutta koskeva riski
    b. ICT:n turvallisuusriski
    c. ICT:n muutosriski
    d. ICT-tiedon eheysriski
    e. ICT:n ulkoistamista koskeva riski

    Kartoitus auttaa toimivaltaisia viranomaisia määrittämään, mitkä riskit ovat (mahdollisesti) olennaisia, jolloin niitä tulisi arvioida tarkemmin ja/tai yksityiskohtaisemmin seuraavassa esitettävissä arviointitoimenpiteissä.

3.3 Olennaisten ICT-riskien vähentämiseksi toteutettavien kontrollien arviointi

45. Arvioidakseen yhtiön ICT-jäännösriskit toimivaltaisten viranomaisten tulisi tarkistaa, miten laitoksessa tunnistetaan, seurataan, arvioidaan ja vähennetään riskejä, jotka toimivaltaiset viranomaiset ovat määrittäneet olennaisiksi edellä esitetyssä arvioinnissa.

46. Tätä varten toimivaltaisten viranomaisten tulisi arvioida havaittujen olennaisten ICT-riskien osalta seuraavat:

    a. ICT-riskien hallintaperiaatteet, prosessit ja riskinsietorajat;
    b. organisaation hallinta- ja valvontajärjestelmä;
    c. sisäisen tarkastuksen kattavuus ja tulokset, sekä
    d. ICT-riskin erityiset valvontajärjestelyt, jotka koskevat havaittua olennaista ICT-riskiä.

47. Arvioinnissa tulisi ottaa huomioon EPV:n SREP-ohjeiden 5 osastossa tarkoitetun yleisen riskienhallinnan ja sisäisen valvonnan järjestelmän analyysin tulokset sekä näiden ohjeiden 2 osastossa käsitelty yhtiön ICT-hallinta ja -strategia, koska näillä osa-alueilla havaitut merkittävät puutteet voivat vaikuttaa yhtiön kykyyn hallita ja vähentää sen ICT-riskejä. Toimivaltaisten viranomaisten tulisi myös tarvittaessa hyödyntää näiden ohjeiden 37 kohdassa tarkoitettuja tietolähteitä.

48. Toimivaltaisten viranomaisten tulisi suorittaa seuraavat arviointitoimenpiteet siten, että ne ovat suhteutettuja yhtiön toimintojen luonteeseen, laajuuteen ja monimuotoisuuteen nähden. Niiden tulisi myös soveltaa yhtiön ICT-riskiprofiilin kannalta tarkoituksenmukaista valvojan arviointimenetelmää.

3.3.1 ICT-riskien hallintaa koskevat toimintaperiaatteet, prosessit ja riskinsietorajat

49. Toimivaltaisten viranomaisten tulisi arvioida, onko laitoksella käytössä riskienhallintaa koskevat asianmukaiset toimintaperiaatteet, prosessit ja riskinsietorajat havaittuja olennaisia ICT-riskejä varten.

Nämä voivat olla osana operatiivisen riskin hallintajärjestelmää tai ne voidaan esittää erillisessä asiakirjassa. Tätä arviointia varten toimivaltaisten viranomaisten tulisi ottaa huomioon seuraavat seikat:

a. ylin hallintoelin on laatinut riskienhallintaa koskevat toimintaperiaatteet viralliseen muotoon ja hyväksynyt ne, ja niihin sisältyy riittävästi ohjeistusta yhtiön ICT-riskinottohalusta ja tärkeimmistä ICT-riskien hallinnan tavoitteista ja/tai ICT-riskeihin sovellettavista sietorajoista. ICT-riskien hallintaperiaatteet tulisi myös toimittaa tiedoksi kaikille sidosryhmille;

b. sovellettavat riskienhallintaperiaatteet kattavat kaikki merkittävät osatekijät havaittujen olennaisten ICT-riskien hallintaa varten;

c. yhtiö on ottanut käyttöön prosessin ja sen perustana olevat menettelytavat tunnistaakseen (esim. riskienvalvonnan itsearviointien ja riskien skenaarioanalyysin avulla) olennaiset ICT-riskit ja seuratakseen niitä, ja

d. yhtiö käyttää ICT-riskien hallintaa koskevaa raportointia, joka tarjoaa ajantasaista tietoa toimivalle johdolle ja ylimmälle hallintoelimelle ja jonka ansiosta toimiva johto ja/tai ylin hallintoelin voi arvioida ja seurata, noudatetaanko yhtiön ICT-riskien vähentämissuunnitelmissa ja -toimenpiteissä hyväksyttyä riskinottohalua ja/tai (mahdollisia) riskinsietorajoja, sekä valvoa olennaisten ICT-riskien muutoksia.

3.3.2 Organisaation hallinta- ja valvontajärjestelmä

50. Toimivaltaisten viranomaisten tulisi arvioida, miten riskienhallintatehtävät ja -vastuut sisällytetään ja integroidaan yhtiön sisäiseen organisaatioon havaittujen olennaisten ICT-riskien hallintaa ja valvontaa varten. Toimivaltaisten viranomaisten tulisi tältä osin arvioida, osoittaako yhtiö, että

a. sillä on selkeät tehtävät ja vastuut olennaisten ICT-riskien tunnistamista, arviointia, seurantaa, vähentämistä, raportointia ja valvontaa varten;

b. riskejä koskevista vastuista ja tehtävistä tiedotetaan selkeästi, ja ne kohdennetaan ja sisällytetään organisaation kaikkiin osiin (esim. liiketoiminta-alueisiin ja tietohallintoon) ja prosesseihin, ja huomioon otetaan myös tehtävät ja vastuut, jotka koskevat riskitietojen keräämistä ja ryhmittelyä ja niiden raportointia toimivalle johdolle ja/tai ylimmälle hallintoelimelle;

c. ICT-riskien hallintatoiminnot suoritetaan siten, että niissä on määrän ja laadun kannalta riittävästi henkilöstöä ja teknisiä resursseja; riskien vähentämissuunnitelmien uskottavuuden arvioimiseksi toimivaltaisten viranomaisten tulisi laatia arvio myös siitä, onko yhtiö osoittanut riittävästi rahoitusta ja/tai tarvittavia resursseja suunnitelmien toteuttamiseen;

d. ylin hallintoelin seuraa riittävästi havaintoja, joita riippumattomat valvontatoiminnot ovat tehneet ICT-riskistä (-riskeistä), ja reagoi niihin sekä ottaa huomioon, että joissakin näkökohdissa vastuu on ehkä siirrettävä toimikunnalle, jos sellainen on olemassa, ja

e. poikkeukset sovellettavista ICT-määräyksistä, ja -toimintaperiaatteista kirjataan ylös, ja riippumaton valvontatoiminto arvioi niitä koskevat asiakirjat ja raportoi niistä keskittyen niihin liittyviin riskeihin.

3.3.3 Sisäisen tarkastuksen kattavuus ja tulokset

51. Toimivaltaisten viranomaisten tulisi selvittää, onko sisäisen tarkastuksen toiminta tehokas ICT-riskien kontrollimenetelmiä koskevissa tarkastuksissa. Tätä varten niiden tulisi arvioida

    a. ovatko ICT-riskien kontrollimenetelmiä koskevat tarkastukset riittävän laadukkaita ja yksityiskohtaisia, suoritetaanko niitä riittävän usein ja ovatko ne oikein suhteutettuja yhtiön kokoon, toimintoihin ja ICT-riskiprofiiliin nähden;

    b. sisältyykö tarkastussuunnitelmaan tarkastuksia, jotka koskevat yhtiön havaitsemia kriittisiä ICT-riskejä;

    c. raportoidaanko sovituista toimista ja muista tärkeistä ICT-tarkastusten tuloksista ylimmälle hallintoelimelle, ja

    d. seurataanko sovittuja toimia ja muita ICT-tarkastusten tuloksia ja arvioiko toimiva johto ja/tai tarkastustoimikunta säännöllisesti väliraportit.

3.3.4 Merkittävät ICT-riskit ja niihin liittyvät kontrollit

52. Toimivaltaisten viranomaisten tulisi arvioida, onko laitoksella havaittuja olennaisia ICT-riskejä koskevat kontrollit. Seuraavissa jaksoissa luetellaan esimerkinomaisesti kontrollit, joita on tarkasteltava arvioitaessa 3.2.3 kohdan mukaisesti tunnistettuja merkittäviä riskejä, jotka on jaettu seuraaviin ICT-riskiluokkiin:

    a. ICT:n saatavuutta ja jatkuvuutta koskevat riskit
    b. ICT:n turvallisuusriskit
    c. ICT:n muutosriskit
    d. ICT-tiedon eheysriskit
    e. ICT:n ulkoistamista koskevat riskit.

(a) ICT:n saatavuutta ja jatkuvuutta koskevien merkittävien riskien kontrollit

53. Toimivaltaisten viranomaisten tulisi arvioida EPV:n SREP-ohjeissa (279–281 kohdassa) asetettujen vaatimusten lisäksi, käyttääkö yhtiö tarkoituksenmukaista toimintamallia, jolla tunnistetaan, ymmärretään, mitataan ja vähennetään ICT:n saatavuutta ja jatkuvuutta koskevia riskejä.

54. Tässä arvioinnissa toimivaltaisten viranomaisten tulisi ottaa huomioon toimintamallista erityisesti seuraavat seikat:

    a. Siinä tunnistetaan kriittiset ICT-prosessit ja niitä tukevat järjestelmät, joiden tulisi olla osa liiketoiminnan jatkuvuutta koskevia suunnitelmia, ja siihen sisältyy

        i. kattava analyysi kriittisten liiketoimintaprosessien ja tukijärjestelmien riippuvuussuhteista;

        ii. kriittisiä prosesseja tukevien tietojärjestelmien palautumistavoitteet (määritys suoritetaan tavallisesti liiketoiminnassa ja/tai määräyksissä palautusaikatavoitteen ja palautuspistetavoitteen avulla);

iii. asianmukainen jatkuvuussuunnitelma, joka mahdollistaa kriittisten ICT-järjestelmien ja -palvelujen saatavuuden, jatkuvuuden ja palautumisen, jotta yhtiön toiminnoille aiheutuisi mahdollisimman vähän häiriöitä siedettävän ajan kuluessa.

b. Siinä on liiketoiminnan häiriönsietokykyä ja jatkuvuuden hallintaympäristöä koskevat toimintaperiaatteet ja vaatimukset sekä kontrollit, joihin sisältyy

i. toimenpiteitä, joilla estetään yksittäisen skenaarion tai häiriö- tai poikkeustilanteen mahdollinen vaikutus sekä ICT:n tuotanto- että varajärjestelmiin;

ii. ICT-järjestelmien varmistus- ja palautusmenettelyt, jotka koskevat kriittisiä ohjelmistoja ja tietoja ja joilla varmistetaan, että varmuuskopiot tallennetaan turvalliseen ja riittävän etäiseen paikkaan, jotta tärkeät tiedot eivät voi tuhoutua tai korruptoitua häiriö- tai hätätilanteessa;

iii. valvontaratkaisuja, joiden avulla ICT:n saatavuutta tai jatkuvuutta koskevat häiriöt voidaan havaita nopeasti;

iv. häiriötilanteiden hallintaa ja eskaloitumista koskeva dokumentoitu prosessi, joka tarjoaa myös ohjeita häiriöitilanteiden hallintaa ja eskaloitumista koskevista eri tehtävistä ja vastuista, kriisitoimikunnan (-toimikuntien) jäsenistä ja johtamisjärjestelyistä hätätilanteissa;

v. konkreettisia toimenpiteitä, joilla sekä suojataan yhtiön kriittinen ICT-infrastruktuuri (esim. datakeskukset) ympäristöriskeiltä (esim. tulvilta ja muilta luonnonkatastrofeilta) että varmistetaan ICT-järjestelmille asianmukainen käyttöympäristö (esim. ilmastointi);

vi. prosesseja, tehtäviä ja vastuita, joilla varmistetaan, että myös ulkoistetut ICT-järjestelmät ja -palvelut kuuluvat liiketoiminnan häiriönsietokykyä ja jatkuvuutta koskevien asianmukaisten ratkaisujen ja suunnitelmien piiriin;

vii. ICT:n suorituskyvyn ja kapasiteetin suunnittelu- ja valvontaratkaisuja, jotka koskevat kriittisiä ICT-järjestelmiä ja -palveluja ja joissa on määritelty saatavuusvaatimuksia, jotta merkittävät suorituskyky- ja kapasiteettirajoitteet voidaan havaita nopeasti;

viii. ratkaisuja, joilla kriittiset internettoiminnot tai -palvelut (esim. sähköiset pankkipalvelut) suojataan tarvittaessa internetissä tapahtuvilta palvelunestohyökkäyksiltä ja muilta kyberhyökkäyksiltä, joiden tavoitteena on estää tällaisten toimintojen ja -palvelujen käyttö tai häiritä sitä.

c. Siinä testataan ICT:n saatavuuden ja jatkuvuuden turvaavia ratkaisuja realistisilla skenaarioilla, kuten kyberhyökkäyksillä, varajärjestelyihin siirtymistä koskevilla testeillä ja kriittisten ohjelmistojen ja tietojen varmuuskopioiden testauksilla,

i. jotka ovat suunniteltuja, muodollisia ja dokumentoituja ja joissa testituloksia käytetään ICT:n saatavuutta ja jatkuvuutta koskevien ratkaisujen tehostamiseksi;

ii. joihin sisältyy organisaation sidosryhmiä ja toimintoja, kuten liiketoiminta-alueiden johtoryhmiä sekä liiketoiminnan jatkuvuudesta, häiriötilanteista ja kriisitoiminnasta vastaavia ryhmiä sekä yhtiön ulkopuolisia sidosryhmiä, jotka kuuluvat ekosysteemiin;

iii. joihin ylin hallintoelin ja toimiva johto osallistuvat asiaankuuluvasti (esim. osana kriisinhallintaryhmää) ja joiden tulokset ilmoitetaan näille.

(b) Merkittävien ICT turvallisuusriskien kontrollit

55. Toimivaltaisten viranomaisten tulisi arvioida, onko laitoksella käytössään tehokas järjestelmä ICT:n turvallisuusriskin tunnistamista, ymmärtämistä, mittaamista ja vähentämistä varten. Tässä arvioinnissa toimivaltaisten viranomaisten tulisi ottaa huomioon erityisesti, onko järjestelmässä kiinnitetty huomiota seuraaviin:

a. Selkeästi määritellyt tehtävät ja vastuut, jotka koskevat
   i. ICT:n päivittäisen turvallisuuden hallinnasta sekä ICT:n yleisten turvallisuusperiaatteiden laadinnasta vastaavaa ja/tai tilintekovelvollista henkilöä (henkilöitä) ja/tai toimikuntia, ja joissa kiinnitetään huomiota heidän/niiden riippumattomuuteen;
   ii. ICT-turvallisuuteen liittyvien kontrollien suunnittelua, toteutusta, hallintaa ja seurantaa;
   iii. kriittisten ICT-järjestelmien ja -palvelujen suojaamista ottamalla käyttöön esimerkiksi haavoittuvuusarviointiprosessi, ohjelmistokorjausten hallintaprosessi, päätelaitteen suojaus (esim. haittaohjelmilta ja viruksilta) sekä tunkeutumisen havaitsemis- ja estovälineet;
   iv. ICT:n turvallisuuteen vaikuttavien yhtiön ulkopuolisten tai sisäisten häiriötapahtumien seurantaa, luokittelua ja käsittelyä, kuten häiriötapahtumiin reagointia sekä ICT-järjestelmien ja -palvelujen jatkumista ja palautumista;
   v. säännöllisiä ja ennakoivia uhka-arvioita asianmukaisten kontrollien ylläpitämiseksi.

b. ICT:n turvallisuusperiaatteet, joissa otetaan huomioon ja tarvittaessa noudatetaan kansainvälisesti tunnustettuja ICT:n turvallisuusstandardeja ja -periaatteita (esim. välttämättömien käyttöoikeuksien periaate (principle of least privilege) eli käyttöoikeuksien rajaaminen suppeimpiin oikeuksiin, jotka mahdollistavat tavanomaisen toiminnan käyttöoikeudenhallinnassa, ja monikerrossuojaamisen (”defence in depth”) periaate, jonka mukaan monitasoiset turvallisuusjärjestelyt lisäävät koko järjestelmän turvallisuutta tietoturva-arkkitehtuuria suunniteltaessa).

c. ICT-järjestelmien ja -palvelujen oikeasuhteisten tietoturvavaatimusten määritysprosessi, jossa otetaan huomioon mahdollinen petosriski ja/tai luottamuksellisten tietojen mahdollinen väärinkäyttö ja/tai laiton käyttö sekä dokumentoidut tietoturvaodotukset, joita on noudatettava tällä tavoin määritettyjen ICT-järjestelmien, -palvelujen ja -tietojen osalta, joissa otetaan huomioon yhtiön riskinottohalu ja joita monitoroidaan niiden moitteettoman toteutuksen varmistamiseksi.

d. Tietoturvahäiriöiden hallintaa ja eskaloitumista koskeva dokumentoitu prosessi, joka antaa myös ohjeita häiriöitilanteiden hallintaa ja eskaloitumista koskevista eri tehtävistä ja vastuista, kriisitoimikunnan (-toimikuntien) jäsenistä ja johtamisjärjestelyistä tietoturvaa koskevissa hätätilanteissa.

e. Käyttäjien ja admin-käyttäjien sisäänkirjautumistietojen kirjaaminen, jotta luvatonta toimintaa voidaan tarkkailla tehokkaasti, se voidaan havaita nopeasti ja siihen voidaan reagoida nopeasti ja jotta voidaan tarjota apua tietoturvahäiriöiden rikostutkinnoissa tai käynnistää niitä. Yhtiöllä tulisi olla käytössään sisäänkirjautumistietoja koskevat toimintaperiaatteet, joissa määritellään ylläpidettävät asianmukaiset lokityypit ja niiden säilytysajat.

f. Valistus- ja tiedotuskampanjat tai -aloitteet, joilla yhtiön kaikille tasoille tiedotetaan yhtiön ICT-järjestelmien turvallisesta käytöstä ja suojaamisesta sekä tärkeimmistä (ja muistakin) ICT:n turvallisuusriskeistä, joista henkilöstön tulisi olla tietoinen. Henkilöstölle tulisi tiedottaa varsinkin nykyisistä ja kehittymässä olevista kyberuhista (esim. tietokoneviruksista, mahdollisista sisäisistä tai ulkoisista väärinkäytöistä tai hyökkäyksistä ja kyberhyökkäyksistä) ja siitä, miten he voivat olla mukana vähentämässä tietoturvaloukkauksia.

g. Riittävät fyysiset turvallisuustoimenpiteet (esim. kameravalvonta, murtohälyttimet ja turvaovet), joilla estetään pääsy kriittisten ja arkaluonteisten ICT-järjestelmien luo (esim. datakeskuksissa).

h. Toimenpiteet, joilla ICT-järjestelmät suojataan internetistä tai muista ulkopuolisista verkoista (esim. perinteiset tietoliikenneyhteydet tai yhteydet luotettaviin kumppaneihin) tulevilta hyökkäyksiltä (esim. kyberhyökkäyksiltä). Toimivaltaisten viranomaisten tulisi arvioida, onko yhtiön toimintamallissa otettu huomioon seuraavat:

    i. Prosessi ja ratkaisut, joilla pidetään yllä täydellistä ja ajantasaista luetteloa ja yhteenvetoa kaikista yhtiön ulkopuolelle suuntautuvista verkon liitäntäpisteistä (esim. verkkosivut, internetsovellukset, WiFi, etäyhteys), joiden kautta kolmannet osapuolet voivat tunkeutua yhtiön sisäisiin ICT-järjestelmiin.

    ii. Tarkasti hallinnoidut ja monitoroidut tietoturvatoimenpiteet (esim. palomuurit, välityspalvelimet, sähköpostin välityspalvelut, virustarkistus- ja sisällön tarkistusohjelmat), jotta voidaan turvata saapuva ja lähtevä verkkoliikenne (esim. sähköposti) ja yhtiön ulkopuolelle suuntautuvat verkkoyhteydet, joiden kautta kolmannet osapuolet voivat tunkeutua yhtiön sisäisiin ICT-järjestelmiin.

    iii. Prosessit ja ratkaisut, joilla suojataan verkkosivustot ja sovellukset, joita voidaan vahingoittaa suoraan internetistä ja/tai yhtiön ulkopuolelta ja joiden kautta voidaan päästä yhtiön sisäisiin ICT-järjestelmiin. Tällaisiin prosesseihin ja ratkaisuihin sisältyy yleensä yhdistelmä tunnettuja turvallisuuden kehittämiskäytäntöjä, ICT-järjestelmien käyttörajoituksia ja haavoittuvuustarkistuksia koskevia käytäntöjä ja/tai sovellusten palomuurien ja/tai tunkeutumisen havaitsemista ja/tai ennaltaehkäisyä koskevien järjestelmien tai muiden ylimääräisten tietoturvaratkaisujen toteutusta.

    iv. Säännöllisin väliajoin suoritettava tietoturvallisuuden penetraatiotestaus, jolla arvioidaan toteutettujen kybertoimenpiteiden ja yhtiön sisäisten ICT:n tietoturvatoimenpiteiden tehokkuus. Tällaisten testien suorittajien tulisi olla riittävän asiantuntemuksen omaavaa henkilöstöä ja/tai ulkopuolisia asiantuntijoita, testitulokset tulisi dokumentoida ja päätelmät ilmoittaa toimivalle johdolle ja/tai ylimmälle hallintoelimelle. Mikäli tarpeen ja mahdollista, yhtiön tulisi hyödyntää tällaisten testien tuloksia parantaakseen turvavalvontaa ja -prosesseja entisestään ja/tai saadakseen paremman varmuuden niiden tehokkuudesta.

(c) Merkittävien ICT -muutosriskien kontrollit

56. Toimivaltaisten viranomaisten tulisi arvioida, onko yhtiöllä käytössään ICT:n muutosriskin tunnistamiseksi, ymmärtämiseksi, mittaamiseksi ja vähentämiseksi tehokas toimintamalli, joka on oikein suhteutettu yhtiön toimintojen luonteeseen, laajuuteen ja monimuotoisuuteen sekä ICT-riskiprofiiliin. Yhtiön toimintamallin tulisi kattaa riskit, jotka liittyvät ICT-järjestelmien muutosten kehittämiseen, testaukseen ja hyväksymiseen, mukaan lukien ohjelmistokehitys tai -muutokset ennen ohjelmistojen siirtämistä tuotantoympäristöön. Toimintamallin tulisi myös varmistaa tietojärjestelmien asianmukainen elinkaarihallinta. Tässä arvioinnissa toimivaltaisten viranomaisten tulisi ottaa huomioon erityisesti, onko toimintamallissa kiinnitetty huomiota seuraaviin:

    a. dokumentoidut prosessit ICT-järjestelmien (esim. järjestelmän hallinta ja korjausten hallinta) ja datan (esim. virheiden tai tietojen korjaukset) muutosten hallintaa ja kontrollointia varten, jotta voidaan varmistaa ICT-riskienhallinnan riittävä osallistuminen tärkeisiin ICT-muutoksiin, jotka voivat vaikuttaa merkittävästi yhtiön riskiprofiiliin tai kokonaisriskiin;

    b. määritelmät, jotka koskevat tehtävien eriyttämisvaatimuksia ICT:n muutosprosessien eri vaiheissa (esim. ratkaisusuunnittelu ja -kehitys, uusien ohjelmistojen ja/tai muutosten testaus ja hyväksyntä, siirtäminen tuotantoympäristöön ja virheiden korjaaminen) ja joissa tulisi keskittyä toteutettuihin ratkaisuihin ja tehtävien eriyttämiseen tarkoituksena hallita ja valvoa ICT-henkilöstön (esim. kehittäjien, ICT-järjestelmien ja tietokannan valvojien) tai muiden tahojen (esim. yrityskäyttäjien ja palveluntarjoajien) tekemiä muutoksia tuotantojärjestelmiin ja tietoihin;

    c. testausympäristöt, joissa otetaan riittävästi huomioon tuotantoympäristöt;

    d. tuotantoympäristössä sekä testaus- ja kehitysympäristössä olevien nykyisten sovellusten ja ICT-järjestelmien ominaisuudet, jotta tarvittavat muutokset (esim. versioiden päivitykset tai parannukset, järjestelmien korjaukset, määritysten muutokset) voidaan asianmukaisesti toteuttaa ja jotta niitä voidaan asianmukaisesti hallita ja valvoa muutoksenalaisissa ICT-järjestelmissä;

    e. prosessi, jolla seurataan ja hallitaan käytettävien ICT-järjestelmien elinkaarta sen varmistamiseksi, että ne täyttävät edelleen tämänhetkiset liiketoiminnan ja riskienhallinnan vaatimukset, että käytettävien ICT-ratkaisujen ja -järjestelmien myyjät tarjoavat niihin edelleen tukea ja että prosessin tukena on asianmukaiset ohjelmistokehityksen elinkaarta koskevat menettelyt;

    f. ohjelmiston lähdekoodin kontrollit, joilla estetään luvattomat muutokset yhtiön sisällä kehitetyn ohjelmiston lähdekoodiin;

    g. prosessi, jolla suoritetaan uusien tai olennaisesti muutettujen ICT-järjestelmien ja ohjelmistojen turva- ja haavoittuvuusseulonta ennen kuin ne otetaan käyttöön tuotannossa ja ennen kuin ne altistuvat mahdollisille kyberhyökkäyksille;

    h. prosessi ja ratkaisut, joilla estetään pääsy luottamuksellisiin tietoihin ICT-järjestelmien korvaamisen, arkistoinnin, käytöstäpoiston tai tuhoamisen yhteydessä;

    i. riippumaton arviointi- ja validointiprosessi, jolla vähennetään ICT-järjestelmiin tehtävien muutosten yhteydessä inhimillisten virheiden riskiä, joka saattaa heikentää merkittävästi yhtiön toimintavalmiutta, toiminnan jatkuvuutta tai tietoturvaa (esim. merkittävät muutokset palomuurimääritykseen tai palomuureihin).

(d) Merkittävien ICT-tiedon eheysriskien kontrollit

57. Toimivaltaisten viranomaisten tulisi arvioida, onko laitoksella käytössään ICT-tiedon eheysriskin tunnistamiseksi, ymmärtämiseksi, mittaamiseksi ja vähentämiseksi tehokas toimintamalli, joka on oikein suhteutettu yhtiön toimintojen luonteeseen, laajuuteen ja monimuotoisuuteen sekä ICT-riskiprofiiliin. Yhtiön toimintamallissa tulisi ottaa huomioon riskit, jotka liittyvät ICT-järjestelmiin tallennetun tai niissä käsitellyn tiedon eheyden säilyttämiseen. Tässä arvioinnissa toimivaltaisten viranomaisten tulisi ottaa huomioon erityisesti, onko toimintamallissa kiinnitetty huomiota seuraaviin:

a. toimintaperiaatteet, joissa määritellään ICT-järjestelmissä olevan tiedon eheyden hallintaa koskevat tehtävät ja vastuut (esim. tietoarkkitehti (data architect), tiedonhallintavastaavat (data officers)[6], tiedon hoitaja (data custodian)[7] data owners/stewards[8]) ja jotka tarjoavat ohjeita siitä, mitkä tiedot ovat tiedon eheyden kannalta kriittisiä ja edellyttävät erityisiä ICT kontrolleja (esim. syötettävän tiedon kelpoisuuden automaattiset tarkistukset, tiedonsiirron valvontajärjestelyt, täsmäytykset jne.) tai tarkastuksia (esim. yhteensopivuustarkastusta tietoarkkitehtuurin kanssa) ICT-tiedon elinkaaren eri vaiheissa;

b. dokumentoitu tietoarkkitehtuuri, tietomalli ja/tai tietohakemisto, jonka liiketoiminnan ja tietotekniikan sidosryhmät validoivat ja jonka tarkoituksena on tukea tarvittavaa tiedon yhtenäisyyttä eri ICT-järjestelmissä sekä varmistaa, että tietoarkkitehtuuri, tietomalli ja/tai tietohakemisto vastaavat liiketoiminnan ja riskienhallinnan tarpeita;

c. toimintaperiaatteet, jotka koskevat itsenäiskäyttöä (End User Computing) ja varsinkin tärkeiden itsenäiskäyttöä koskevien ratkaisujen määrittämistä, rekisteröintiä ja dokumentointia (esim. tärkeiden tietojen käsittelyn yhteydessä), sekä odotetut turvallisuustasot luvattomien muutosten estämiseksi sekä itse välineessä että siihen tallennetuissa tiedoissa;

d. poikkeusten käsittelyä koskevat dokumentoidut prosessit, joilla ratkotaan ICT-tiedon eheydessä havaittuja ongelmia tietojen tärkeyden ja arkaluonteisuuden mukaan.

58. Jos valvottavat yhtiöt kuuluvat riskidatan tehokasta aggregointia ja riskiraportointia koskevien Baselin pankkivalvontakomitean BCBS 239-periaatteiden piiriin[9], toimivaltaisten viranomaisten tulisi arvioida yhtiön tekemä riskianalyysi riskiraportointia ja datan aggregointia koskevista valmiuksistaan vertaamalla niitä periaatteisiin ja niitä koskeviin asiakirjoihin. Tällöin tulisi ottaa huomioon periaatteiden toteutusaikataulu ja siirtymäjärjestelyt.

(e) ICT:n ulkoistamista koskevien merkittävien riskien kontrollit

59. Toimivaltaisten viranomaisten tulisi arvioida, sovelletaanko yhtiön ulkoistamisstrategiassa ulkoistamisesta annettujen Euroopan pankkivalvontaviranomaisten komitean (CEBS) ohjeiden

[6] Tiedonhallintavastaava vastaa tiedon käsittelystä ja käytöstä.

[7] Tiedon hoitaja vastaa tiedon turvallisesta huollosta, siirrosta ja tallennuksesta.

[8] Data steward vastaa tietoelementtien – sekä sisällön että metadatan – hallinnasta ja käyttökelpoisuudesta.

[9] Baselin pankkivalvontakomitea, Principles for effective risk data aggregation and risk reporting, tammikuu 2013, saatavilla osoitteessa: http://www.bis.org/publ/bcbs239.pdf.

vaatimusten mukaisesti ja lisäksi EPV:n SREP-ohjeiden 85 kohdan d alakohdan vaatimuksen mukaisesti riittävästi kyseisiä vaatimuksia ICT:n ulkoistamiseen, myös ryhmän sisällä tapahtuvaan ryhmän sisäisten ICT-palvelujen ulkoistamiseen. ICT:n ulkoistamista koskevia riskejä arvioidessaan toimivaltaisten viranomaisten tulisi ottaa huomioon, että ICT:n ulkoistamista koskevat riskit voidaan arvioida myös osana EPV:n SREP-ohjeiden 240 kohdan j alakohdassa esitettyä laitokselle ominaisen operatiivisen riskin arviointia. Näin voidaan välttää päällekkäisyydet tai kahdenkertaiset laskutoimitukset.

60. Toimivaltaisten viranomaisten tulisi arvioida erityisesti, onko laitoksella käytössään ICT:n ulkoistamista koskevan riskin tunnistamiseksi, ymmärtämiseksi ja mittaamiseksi tehokas toimintamalli ja erityisesti kontrollit ja kontrolliympäristö, joilla voidaan vähentää ulkoistettuja olennaisia ICT-palveluja koskevia riskejä ja jotka ovat oikein suhteutettuja yhtiön kokoon, toimintaan ja ICT-riskiprofiiliin. Toimintamallissa tulisi olla seuraavat:

   a. Arviointi ICT:n ulkoistamisen vaikutuksesta yhtiön riskienhallintaan, joka koskee palveluntarjoajien käyttöä (esim. pilvipalvelujen tarjoajat) ja niiden tarjoamia palveluja hankintaprosessissa. Arviointi on dokumentoitava, ja toimivan johdon tai ylimmän hallintoelimen tulisi ottaa se huomioon tehdessään päätöstä palvelujen ulkoistamisesta. Yhtiön tulisi arvioida ICT-riskien hallintaperiaatteet, ICT:n valvontajärjestelyt ja palveluntarjoajan valvontaympäristö varmistaakseen, että ne vastaavat yhtiön sisäisiä riskienhallintatavoitteita ja riskinottohalua. Tämä arvio tulisi päivittää säännöllisin väliajoin sopimuksellisen ulkoistamisen aikana ottaen huomioon ulkoistettujen palvelujen ominaispiirteet.

   b. Ulkoistettuihin palveluihin liittyvien ICT-riskien seuranta sopimuksellisen ulkoistamisen aikana osana yhtiön riskienhallintaa, ja seurantatietojen sisällyttäminen yhtiön ICT-riskien hallintaa koskevaan raportointiin (esim. liiketoiminnan jatkuvuutta koskeva raportointi, turvallisuusraportointi).

   c. Palvelutasojen määrän seuranta ja vertaaminen sopimuksissa sovittuihin palvelutasoihin. Tämän tulisi olla osa ulkoistamissopimusta tai palvelutasosopimusta.

   d. Riittävästi henkilöstöä, resursseja ja toimivaltuuksia ulkoistetuista palveluista johtuvien ICT-riskien seurantaa ja hallintaa varten.

3.4 Yhteenveto havainnoista ja pisteytys

61. Toimivaltaisten viranomaisten tulisi muodostaa edellä esitetyn arvioinnin perusteella näkemys yhtiön ICT-riskeistä. Tämä näkemys tulisi sisältyä havaintoyhteenvetoon, joka toimivaltaisten viranomaisten tulisi ottaa huomioon laatiessaan operatiivista riskiä koskevaa pisteytystä EPV:n SREP-ohjeiden taulukkoon 6. Toimivaltaisten viranomaisten tulisi perustaa näkemyksensä olennaisiin ICT-riskeihin ja ottaa huomioon seuraavat operatiivisen riskin arviointiin sisällytettävät näkökohdat:

   a. Riskiä koskevat näkökohdat

      i. yhtiön ICT-riskiprofiili ja ICT-riskit,
      ii. kriittisiksi määritetyt ICT-järjestelmät ja -palvelut, ja
      iii. kriittisiä ICT-järjestelmiä koskevan ICT-riskin olennaisuus.

b. Riskien hallintaa ja kontrolleja koskevat näkökohdat

i. yhtiön riskienhallintaperiaatteet ja strategia ovat yhdenmukaiset yhtiön kokonaisstrategian ja riskinottohalun kanssa;
ii. ICT-riskien hallinnan organisaatiokehys on vankka, siinä on selkeät vastuualueet, ja riskien omistajien, johdon sekä riskienhallinnan tehtävät on erotettu selkeästi;
iii. ICT-riskien mittaamis-, seuranta- ja raportointijärjestelmät ovat asianmukaiset, ja
iv. ICT-riskien valvontajärjestelmä on luotettava.

62. Jos toimivaltaiset viranomaiset pitävät ICT-riskiä merkittävänä ja päättävät arvioida ja pisteyttää sen operatiivisen riskin alaluokkana, niiden tulisi ottaa huomioon ICT-riskin pisteytystä koskevat näkökohdat, jotka esitetään seuraavassa taulukossa (Taulukko 1).

Taulukko 1: Valvontaan perustuvat näkökohdat ICT-riskin pisteyttämistä varten

Riskin pistemäärä	Valvontaan perustuva käsitys	Riskitasoa koskevat näkökohdat	Riittävää hallintaa & valvontajärjestelyjä koskevat näkökohdat
1	Toimintariskin sekä riskienhallinnan ja kontrollien perusteella ei ole havaittavissa riskiä huomattavasta vaikutuksesta yhtiön vakavaraisuuteen.	• Edellä 37 kohdan mukaisesti tarkasteltavat tietolähteet eivät ole tuoneet esiin merkittäviä ICT-riskejä. • Yhtiön ICT-riskiprofiilin luonne yhdessä kriittisiä ICT-järjestelmiä sekä ICT-järjestelmiin ja -palveluihin kohdistuvia olennaisia ICT-riskejä koskevan arvion kanssa ei ole tuonut esiin olennaisia ICT-riskejä.	• Yhtiön ICT-riskejä koskevat toimintaperiaatteet ja strategia ovat oikein suhteutettuja sen kokonaisstrategiaan ja riskinottohaluun. • ICT-riskejä koskeva organisaatiokehys on vankka, siinä on selkeät vastuualueet, ja riskinottajien ja hallinta- ja valvontatoimintojen
2	Yhtiöön kohdistuvan merkittävän vakavaraisuusvaikutuksen riski on alhainen, kun otetaan huomioon riskitaso sekä kontrollit.	• Edellä 37 kohdan mukaisesti tarkasteltavat tietolähteet eivät ole tuoneet esiin merkittäviä ICT-riskejä. • Yhtiön ICT-riskiprofiilin luonne yhdessä kriittisiä ICT-järjestelmiä sekä ICT-järjestelmiin ja -palveluihin kohdistuvia olennaisia ICT-riskejä koskevan arvion kanssa on tuonut esiin alhaisen ICT-riskin (esim. enintään kahdessa viidestä ennalta määritellyistä ICT-	

		riskiluokista).	tehtävät on erotettu selkeästi. • ICT-riskien mittaamis-, seuranta- ja raportointijärjestelmät ovat asianmukaiset. • ICT-riskejä koskeva valvontajärjestelmä on luotettava.
3	Yhtiöön kohdistuvan merkittävän vakavaraisuusvaikutuksen riski on keskimääräinen, kun otetaan huomioon riskitaso sekä kontrollit.	• Edellä 37 kohdan mukaisesti tarkasteltavat tietolähteet ovat tuoneet esiin merkkejä mahdollisista merkittävistä ICT-riskeistä. • Yhtiön ICT-riskiprofiilin luonne yhdessä kriittisiä ICT-järjestelmiä sekä ICT-järjestelmiin ja -palveluihin kohdistuvia olennaisia ICT-riskejä koskevan arvion kanssa on tuonut esiin suurentuneen ICT-riskin (esim. kolmessa viidestä ennalta määritellyistä ICT-riskiluokista).	
4	Yhtiöön kohdistuvan merkittävän vakavaraisuusvaikutuksen riski on suuri, kun otetaan huomioon riskitaso sekä hallinta ja valvontajärjestelyt.	• Edellä 37 kohdan mukaisesti tarkasteltavat tietolähteet ovat tuoneet esiin runsaasti merkkejä merkittävistä ICT-riskeistä. • Yhtiön ICT-riskiprofiilin luonne yhdessä kriittisiä ICT-järjestelmiä sekä ICT-järjestelmiin ja -palveluihin kohdistuvia olennaisia ICT-riskejä koskevan arvion kanssa on tuonut esiin suuren ICT-riskin (esim. neljässä viidestä ennalta määritellyistä ICT-riskiluokista).	

Liite – ICT-riskiluokitus

5 ICT-riskiluokat sekä esimerkinomainen luettelo ICT-riskeistä, jotka ovat vakavuusasteeltaan mahdollisesti suuria ja/tai niillä on suuri operatiivinen, mainetta koskeva tai taloudellinen vaikutus

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
ICT:n saatavuutta ja jatkuvuutta koskevat riskit	Riittämätön kapasiteetinhallinta	Puutteelliset resurssit (esim. laitteistot, ohjelmistot, henkilöstö, palveluntarjoajat) voivat johtaa siihen, ettei palvelua kyetä mitoittamaan liiketoiminnan tarpeisiin, järjestelmähäiriöihin, palvelun huononee ja/tai tehdään operatiivisia virheitä.	• Kapasiteettivaje saattaa heikentää siirtonopeutta ja verkon (internetin) käytettävyyttä internetpankkitoimintoihin ja muihin palveluihin. • Henkilöstövaje (yhtiön sisäinen tai kolmas osapuoli) voi johtaa järjestelmähäiriöihin ja/tai operatiivisiin virheisiin.
	ICT-järjestelmähäiriöt	Käytettävyyden menettäminen laitteistohäiriöiden vuoksi.	• Tallennuksen (kovalevyjen), serverin tai muun ICT-laitteiston häiriöt/viat, jotka johtuvat esim. puutteellisesta ylläpidosta.
		Käytettävyyden menettäminen ohjelmistohäiriöiden ja -virheiden vuoksi.	• Päättymätön silmukka sovellusohjelmistossa estää transaktion suorittamisen. • Katkokset, jotka johtuvat edelleen käytössä olevista vanhentuneista ICT-järjestelmistä ja -ratkaisuista, jotka eivät enää täytä nykyisiä käytettävyys- ja häiriönsietovaatimuksia ja/tai niihin ei enää saada myyjän tukea.
	Riittämätön ICT:n jatkuvuuden ja vakavasta virhetilanteesta palautumisen suunnittelu	ICT:n suunnitellun käytettävyyden ja/tai jatkuvuutta koskevien ratkaisujen ja/tai vakavasta virhetilanteesta palautumisen epäonnistuminen (esim. datakeskuksen varalaitteiston käytöstä toipuminen) häiriötilanteessa.	• Ensisijaisen ja toissijaisen datakeskuksen väliset kokoonpanoerot saattavat johtaa varalla olevan datakeskuksen kyvyttömyyteen turvata palvelun jatkuvuus suunnitellusti.

[10] ICT-riskit luetellaan siinä riskiluokassa, joihin ne vaikuttavat eniten, mutta ne saattavat vaikuttaa myös muihin riskiluokkiin

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
	Toiminta-katkoksia ja tuhoja aiheuttavat kyberhyökkäykset	Eri tarkoituksissa tehdyt hyökkäykset (esim. aktivismi, kiristys), jotka johtavat järjestelmien ja verkon ylikuormittumiseen ja estävät sähköisten laskentapalvelujen laillisia käyttäjiä käyttämästä niitä.	• Hajautettuja palvelunestohyökkäyksiä tehdään hakkereiden kaappaamien lukuisten tietokonejärjestelmien avulla internetissä lähettämällä suuria määriä luotettavilta vaikuttavia palvelupyyntöjä internet-palveluihin (esim. sähköinenpankkitoiminta) .
ICT:n turvallisuusriskit	Kyberhyökkäykset ja muut ICT-pohjaiset hyökkäykset yhtiön ulkopuolelta	Internetistä tai yhtiön ulkopuolisista verkoista tehdyt hyökkäykset eri tarkoituksissa (esim. petokset, vakoilu, aktivismi/sabotaasi, kyberterrorismi) ja eri tekniikoilla (esim. käyttäjän manipulointi, tunkeutumisyritykset haavoittuvuuksia hyödyntämällä, haittaohjelmien käyttö), mikä johtaa sisäisten ICT-järjestelmien haltuun ottamiseen.	Erityyppisiä hyökkäyksiä: • Edistynyt pitkäkestoinen uhka, joka koskee sisäisten järjestelmien haltuun ottamista tai tietojen anastamista (esim. identiteettivarkauden yhteydessä tapahtuva luottokorttitietojen ja muiden tietojen anastaminen). • Haittaohjelmat (esim. kiristysohjelmat), jotka salaavat tiedot kiristystarkoituksessa. • Troijan hevosten tartuttaminen sisäisiin ICT-järjestelmiin tarkoituksena tehdä järjestelmää haittaavia toimia salaisesti. • ICT-järjestelmän ja/tai (verkko)sovellusten haavoittuvuuksien hyödyntäminen (esim. SQL-injektiojne.) tarkoituksena päästä sisäiseen ICT-järjestelmään.
		Hakkereiden tekemät vilpilliset maksutapahtumat, jotka suoritetaan murtamalla tai kiertämällä sähköisten pankki- ja maksupalvelujen tietoturva ja/tai hyökkäämällä ja hyödyntämällä yhtiön sisäisten maksujärjestelmien tietoturvahaavoittuvuuksia .	• Sähköisiin pankkipalveluihin tai maksupalveluihin kohdistuvat hyökkäykset, joiden tarkoituksena on tehdä luvattomia transaktioita. • Vilpillisten maksutapahtumien luominen ja lähettäminen ulos yhtiön sisäisistä maksujärjestelmistä (esim. vilpilliset SWIFT-viestit).
		Vilpilliset arvopaperikaupat, joita hakkerit suorittavat murtamalla tai kiertämällä sellaisten sähköisten pankkipalvelujen tietoturvan, joiden kautta on pääsy myös asiakkaiden arvopaperitileille.	• Niin sanotut pump and dump -hyökkäykset, joissa hakkerit pääsevät sähköisessä pankkitoiminnassa asiakkaille tarjottaville arvopaperitileille ja tekevät vilpillisiä osto- tai myyntimääräyksiä vaikuttaakseen markkinahintoihin ja/tai tekevät voittoa

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
			arvopapereille aiemmin avatuilla positioilla.
		Hyökkäykset viestintäyhteyksiin ja kaikenlaisiin keskusteluihin tai ICT-järjestelmiin tarkoituksena kerätä tietoja ja/tai tehdä petoksia.	• Salakuuntelu tai selväkielitekstinä lähetettyjen suojaamattomien todennustietojen sieppaaminen.
	ICT:n riittämätön sisäinen turvallisuus	Luvaton tunkeutuminen kriittisiin ICT-järjestelmiin yhtiön sisällä eri tarkoituksissa (esim. petokset, luvattoman kaupankäynnin suorittaminen ja salaaminen, tietovarkaudet, aktivismi/sabotaasi) ja monilla eri tekniikoilla (esim. käyttämällä väärin ja/tai laajentamalla käyttöoikeuksia, identiteettivarkauksilla, käyttäjän manipuloinnilla, hyödyntämällä ICT-järjestelmien haavoittuvuuksia ja käyttämällä haittaohjelmia).	• Näppäinpainalluksia tallentavien ohjelmien asentaminen käyttäjätunnuksien ja salasanojen anastamiseksi tarkoituksena käyttää luvattomasti luottamuksellisia tietoja ja/tai tehdä petoksia. • Heikkojen salasanojen murtaminen/arvaaminen luvattomien tai laajempien käyttöoikeuksien hankkimiseksi. • Järjestelmävalvoja käyttää käyttöjärjestelmiä tai tietokannan apuohjelmia (tehdäkseen muutoksia suoraan tietokantaan) vilpillisessä tarkoituksessa.
		ICT:n luvaton muuntelu riittämättömien ICT:n käyttöoikeusmenettelyjen ja -käytäntöjen vuoksi.	• Tarpeettomien tilien sulkemisen tai poistamisen laiminlyönti esim. henkilöstön vaihtaessa tehtäviä ja/tai jättäessä yhtiön tai kun alihankkijat eivät enää tarvitse käyttöoikeuksia, mikä mahdollistaa luvattoman tunkeutumisen ICT-järjestelmiin. • Liian laajojen käyttöoikeuksien myöntäminen, mikä mahdollistaa luvattoman käytön ja/tai mahdollistaa epärehelliset toimet.
		Tietoturvauhat, jotka johtuvat turvallisuustietoisuuden puutteesta, kun työntekijät eivät ymmärrä tai noudata ICT:n turvaperiaatteita ja -menettelyjä tai lyövät ne laimin.	• Työntekijät, jotka harhautetaan antamaan apua hyökkäyksessä (esim. käyttäjän manipulointi). • Tunnistetietoja koskevat huonot käytännöt: salasanojen jakaminen, helposti arvattavien salasanojen käyttäminen, saman salasanan käyttäminen moniin eri tarkoituksiin jne. • Salaamattomien luottamuksellisten tietojen tallentaminen kannettaviin tietokoneisiin ja siirrettäviin tiedontallennusratkaisuihin (esim. USB-muistitikuille), jotka voidaan kadottaa tai varastaa.

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
		Luottamuksellisten tietojen luvaton tallentaminen tai siirtäminen yhtiön ulkopuolelle.	• Henkilöt, jotka varastavat tai vuotavat tarkoituksellisesti tai vievät laitoksesta salaa tietoja valtuudettomille tai muille ulkopuolisille henkilöille.
	ICT:n riittämätön fyysinen turvallisuus	ICT-omaisuuden väärinkäyttö tai anastaminen murtautumalla ICT-laitteisiin fyysisesti aiheuttaen vahinkoja, menetettyä omaisuutta tai tietoja tai mahdollistamalla muut uhat.	• Fyysinen murtautuminen toimistorakennuksiin ja/tai datakeskuksiin ICT-laitteiden (esim. tietokoneiden, kannettavien tai tallennusratkaisujen) anastamiseksi ja/tai tietojen kopioimiseksi pääsemällä fyysisesti ICT-järjestelmien luo.
		Tarkoituksellinen tai tahaton fyysisen ICT-omaisuuden vahingoittaminen terrorismin, onnettomuuksien tai yhtiön henkilöstön ja/tai kolmansien osapuolten (alihankkijoiden, korjaajien) epäonnistuneiden/virheellisten käsittelytoimenpiteiden vuoksi.	• Fyysisen terrorismi (esim. pommi-iskut) tai ICT-omaisuuden sabotointi. • Datakeskuksen tuhoutuminen tulipalon, vesivahingon tai muiden tekijöiden vuoksi.
		Riittämätön fyysinen suojautuminen luonnonkatastrofeilta, mikä johtaa ICT-järjestelmien/datakeskusten osittaiseen tai täydelliseen tuhoutumiseen luonnonkatastrofeissa.	• Maanjäristykset, helleaallot, myrskytuulet, voimakkaat lumimyrskyt, tulvat, tulipalot, ukkosmyrskyt.
ICT:n muutosriskit	ICT-järjestelmien muutosten ja kehittämistyön riittämätön valvonta	Muutosten aiheuttamat virheet tai haavoittuvuudet, jotka jäävät havaitsematta ja aiheuttavat häiriöitä (esim. muutosten odottamattomat vaikutukset tai muutosten huono hallinta riittämättömän testauksen tai virheellisten muutostenhallintakäytäntöjen vuoksi) esim. ohjelmistoihin, ICT-järjestelmiin ja tietoihin.	• Tuotannossa otetaan käyttöön uusia, riittämättömästi testattuja ohjelmistoja tai kokoonpanomuutoksia, joilla on odottamattomia haittavaikutuksia tietoihin (esim. tietojen korruptoituminen tai poistaminen) ja/tai ICT-järjestelmien suorituskykyyn (esim. järjestelmän kaatuminen tai suorituskyvyn heikkeneminen). • ICT-järjestelmiin tai tuotantoympäristössä oleviin tietoihin tehdään muutoksia, joita ei valvota. • Tuotannossa otetaan käyttöön heikosti suojattuja ICT-järjestelmiä ja internetsovelluksia, mikä luo hakkereille tilaisuuksia hyökätä yhtiön tarjoamiin internetpalveluihin ja/tai murtautua yhtiön sisäisiin

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
			ICT-järjestelmiin. • Yhtiön sisällä kehitettyjen ohjelmistojen lähdekoodin hallitsemattomat muutokset. • Riittämätön testaus asianmukaisen testiympäristön puuttumisen vuoksi.
	Riittämätön ICT-arkkitehtuuri	ICT-arkkitehtuurin heikko hallinta ICT-järjestelmien (esim. ohjelmistojen, laitteistojen ja tietojen) suunnittelun, kehittämisen ja ylläpidon yhteydessä voi johtaa ajan mittaan monimutkaisiin, vaikeisiin, kalliisti hallinnoitaviin ja joustamattomiin ICT-järjestelmiin, jotka eivät enää vastaa riittävästi liiketoiminnan tarpeita ja eivätkä täytä riskienhallinnan todellisia vaatimuksia.	• Riittämättömästi hallitut ja pitkään vievät muutokset ICT-järjestelmiin, ohjelmistoihin ja/tai tietoihin, mikä johtaa monimutkaisiin, epäyhtenäisiin ja vaikeasti hallittaviin ICT-järjestelmiin ja -arkkitehtuureihin aiheuttaen monia haittavaikutuksia liiketoiminnan ja riskien hallintaan (esim. riittämätön joustavuus ja ketteryys, ICT:n häiriö- ja vikatilanteet, korkeat käyttökustannukset, ICT:n tietoturvan ja häiriönsietokyvyn heikkeneminen, tietojen laadun ja raportointivalmiuksien heikkeneminen). • Kaupallisten ohjelmistopakettien liiallinen räätälöinti ja laajentaminen yhtiön sisäisesti kehitettyjen ohjelmistojen kanssa, minkä vuoksi kaupallisten ohjelmistojen tulevia julkaisuversioista ei voida ottaa käyttöön ja riski myyjän tuen loppumisesta kasvaa.
	Elinkaaren ja korjausten riittämätön hallinta	Ei kyetä pitämään yllä riittävää ICT-omaisuusluetteloa, joka tukee ja täydentää elinkaaren ja korjausten moitteettomia hallintakäytäntöjä. Tämä johtaa riittämättömästi korjattuihin (ja siten haavoittuvampiin) ja vanhentuneisiin ICT-järjestelmiin, jotka eivät ehkä tue liiketoiminnan ja riskien hallintatarpeita.	• Korjaamattomat ja vanhentuneet ICT-järjestelmät, jotka saattavat vaikuttaa haitallisesti liiketoiminnan ja riskien hallintaan (esim. joustavuuden ja ketteryyden puute, ICT:n käyttökatkokset, ICT:n turvallisuuden ja häiriönsietokyvyn heikkeneminen).
ICT-tiedon eheysriskit	ICT-tiedon prosessoinnin tai käsittelyn	Järjestelmässä, tiedonsiirrossa ja/tai sovelluksissa ilmenevät virheet tai häiriöt tai virheellisesti suoritettu tiedon poiminta-, siirto- ja latausprosessi (extraction,	• IT-järjestelmävirhe eräkäsittelyssä, mikä aiheuttaa virheellisiä saldoja asiakkaan pankkitileillä. • Väärin suoritetut kyselyt.

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
	häiriöt	transfer and load process, ETL) voivat johtaa tietojen korruptoitumiseen tai menettämiseen.	• Tietojen menetys niiden replikoinnissa (varmuuskopioinnissa) ilmenevän virheen vuoksi.
	Huonosti suunnitellut kontrollit tietojen validoinnissa ICT-järjestelmissä	Virheet, jotka liittyvät puuttuvaan tai tehottomaan tietojen automaattista syöttöä ja hyväksymistä koskeviin kontrolleihin (esim. kolmansien osapuolten tietoihin käytettävät), tiedon siirtoa, käsittelyä ja saatuja tietoja koskeviin kontrolleihin ICT-järjestelmissä (esim. syöttötietojen kelpuutusta koskevat kontrollit ja tietojen täsmäytykset).	• Syöttötietojen riittämätön tai virheellinen alustaminen/kelpuutus sovelluksissa ja/tai käyttöliittymissä. • Saatujen tietojen (output data) täsmäytystä koskevien kontrollien puuttuminen • Suoritettujen tiedonpoimintaprosessien (esim. tietokantakyselyjen) kontrollien puuttuminen, mikä johtaa virheellisiin tietoihin. • Yhtiön ulkopuolelta saatujen virheellisten tietojen käyttö.
	Huonosti kontrolloidut tietomuutokset tuotannon ICT-järjestelmissä	Tietoihin päätyy virheitä, koska tuotannon ICT-järjestelmiin tehtyjen tietomuutosten virheettömyyttä ja aiheellisuutta ei valvota .	• Järjestelmien kehittäjät tai tietokantojen admin-käyttäjät pääsevät suoraan ja ilman valvontaa käyttämään ja muuttamaan tuotannossa käytettävien ICT-järjestelmien tietoja esimerkiksi ICT:n häiriötilanteessa.
	Huonosti suunnitellut ja/tai hallitut tietoarkkitehtuurit, tietovuot, tietomallit tai tietohakemistot	Huonosti hallitut tietoarkkitehtuurit, tietomallit, tietovuot tai tietohakemistot voivat johtaa siihen, että samoista tiedoista on monta eri versiota eri ICT-järjestelmissä, jotka eivät ole enää yhdenmukaisia eri tavoilla käytettyjen tietomallien tai tietomääritelmien vuoksi ja/tai erot tietojen luonti- ja muutosprosessissa.	• Tietystä tuotteesta tai liiketoimintayksiköstä on olemassa erilaisia asiakastietokantoja, joissa käytetään erilaisia tietomääritelmiä ja tietokenttiä, mikä johtaa täsmäyttämättömiin ja vaikeasti verrattaviin ja integroitaviin asiakastietoihin koko rahoitusyhtiön tai ryhmän tasolla.
ICT:n ulkoistamista koskevat riskit	Kolmannen osapuolen tai ryhmän jonkin toisen yksikön tarjoamien palvelujen puuteellinen häiriönsietokyky	Kriittiset ulkoistetut ICT-palvelut, tietoliikennepalvelut ja apuohjelmat eivät ole käytettävissä. Kolmannelle osapuolelle uskottujen kriittisten/arkaluonteisten tietojen menetys tai korruptoituminen	• Keskeiset palvelut eivät ole käytettävissä toimittajien (ulkoistetuissa) ICT-järjestelmissä tai -sovelluksissa ilmenevien virheiden vuoksi. • Tietoliikenneyhteyksien katkeaminen. • Häiriö sähkönsaannissa.

ICT-riskiluokat	ICT-riskit (esimerkkejä[10])	Riskin kuvaus	Esimerkkejä
	Ulkoistamisen riittämätön hallinta	Palvelun merkittävä heikkeneminen tai merkittävät häiriöt ulkoistetun palvelun tuottajan heikon varautumisen tai tehottomien kontrollien vuoksi. Ulkoistamisen tehoton hallinta saattaa johtaa siihen, ettei yhtiöllä ole asianmukaista osaamista ja asianmukaisia valmiuksia ICT-riskien täydelliseen tunnistamiseen, arviointiin, vähentämiseen ja seurantaan, ja saattaa heikentää yhtiön toimintavalmiutta.	• Heikot häiriötilanteiden selvitysmenettelyt, sopimusten valvontamekanismit ja palveluntarjoajan sopimukseen sisällytetyt takeet, jotka lisäävät riippuvuutta kolmansista osapuolista ja myyjistä. • Palveluntarjoajan ICT-ympäristöä koskevat puutteelliset muutoksenhallinnan kontrollit, voivat aiheuttaa palvelun merkittävää heikkenemistä tai häiriytymistä.
	Kolmannen osapuolen tai ryhmän jonkin toisen yksikön puuteellinen tietoturva	Murtautuminen ulkopuolisten palveluntarjoajien ICT-järjestelmiin, millä on suora vaikutus ulkoistettuihin palveluihin tai palveluntarjoajan järjestelmiin tallennettuihin kriittisiin/luottamuksellisiin tietoihin. Palveluntarjoajan henkilöstö pääsee käyttämään luvattomasti kriittisiä/arkaluonteisia tietoja, jotka on tallennettu palveluntarjoajan järjestelmiin	• Rikolliset tai terroristit murtautuvat palveluntarjoajien järjestelmiin päästäkseen yhtiöiden ICT-järjestelmiin tai saadakseen käyttöönsä tai tuhotakseen kriittisiä tai arkaluonteisia tietoja, jotka on tallennettu palveluntarjoajan järjestelmiin. • Palveluntarjoajan epärehelliset työntekijät yrittävät anastaa tai myydä arkaluonteisia tietoja.