EBA/GL/2017/05

11/09/2017

Suunised

Suunised info- ja kommunikatsioonitehnoloogia riskide hindamise kohta järelevalvealase läbivaatamise ja hindamise protsessi raames

1. Järgimis- ja aruandluskohustus

Käesolevate suuniste staatus

1. Käesolev dokument sisaldab määruse (EL) nr 1093/2010[1] artikli 16 kohaselt väljastatud suuniseid. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused ja finantseerimisasutused võtma mis tahes meetmeid, et suuniseid järgida.

2. Suunistes esitatakse Euroopa Pangandusjärelevalve seisukoht nõuetekohase järelevalvetava kohta Euroopa Finantsjärelevalve Süsteemis, ehk kuidas tuleks liidu õigust konkreetses valdkonnas kohaldada. Suuniste adressaadiks olevad määruse (EL) nr 1093/2010 artikli 4 punktis 2 määratletud pädevad asutused peaksid suuniseid järgima, kaasates need sobival viisil oma järelevalvetavadesse (nt muutes oma õigusraamistikku või järelevalvemenetlusi) ka siis, kui suunised on mõeldud eelkõige finantseerimisasutustele.

Aruandluskohustus

3. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama EBA-le 13.11.2017, kas nad järgivad või kavatsevad järgida kõnealuseid suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei saada, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleks saata EBA veebisaidil avaldatud vormil aadressil compliance@eba.europa.eu, märkides viite EBA/GL/2017/05. Teate peaksid saatma isikud, kes on asjakohaselt volitatud esitama oma pädeva asutuse nimel nõuete järgimise teateid. Nõuete järgimise staatuse mis tahes muutusest tuleb EBA-le teada anda.

4. Kooskõlas EBA määruse artikli 16 lõikega 3 avaldatakse teated Euroopa Pangandusjärelevalve veebilehel.

[1] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, 24. november 2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).

2. Sisu, kohaldamisala ja mõisted

Sisu ja kohaldamisala

5. Käesolevate direktiivi 2013/36/EL[2] artikli 107 lõike 3 kohaselt koostatud suuniste eesmärk on tagada järelevalvetavade lähendamine info- ja kommunikatsioonitehnoloogia (IKT) riski hindamisel järelevalvealase läbivaatamise ja hindamise protsessi (SREP) raames, millele on osutatud direktiivi 2013/36/EL artiklis 97 ja mida on täpsemalt kirjeldatud EBA suunistes järelevalvealase läbivaatamise ja hindamise protsessi ühise menetluse ning metoodikate kohta[3]. Eelkõige esitatakse käesolevates suunistes hindamiskriteeriumid, mida pädevad asutused peaksid kohaldama krediidiasutuste ja investeerimisühingute IKT valdkonna juhtimise ja strateegia ning oma IKT-riskide suuruse ja kontrollimeetmete järelevalvealasel hindamisel. Käesolevad suunised on EBA järelevalvealase läbivaatamise ja hindamise protsessi suuniste (SREPi suuniste) lahutamatu osa.

6. Pädevad asutused peaksid kohaldama käesolevaid suuniseid kooskõlas järelevalvealase läbivaatamise ja hindamise protsessi rakendamise tasemega, nagu on ette nähtud EBA SREPi suunistes, järgides selles esitatud minimaalse sekkumise mudelit ja proportsionaalsuse nõudeid.

Adressaadid

7. Suunised on adresseeritud määruse (EL) nr 1093/2010 artikli 4 lõike 2 punktis i määratletud pädevatele asutustele.

Mõisted

8. Kui ei ole sätestatud teisiti, on suunistes kasutatud ja määratletud mõistetel sama tähendus kui direktiivis 2013/36/EL, määruses (EL) nr 575/2013 ja EBA suunistes järelevalvealase läbivaatamise ja hindamise protsessi kohta. Peale selle kasutatakse käesolevates suunistes järgmisi mõisteid:

IKT-süsteemid	IKT-kogum kui osa mehhanismist või omavahel ühendatud võrgustikust, mis toetab krediidiasutuse või investeerimisühingu tegevusi.
IKT-teenused	IKT-süsteemide poolt ühele või mitmele sise- või väliskasutajale pakutavad teenused, näiteks andmete

[2] Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (1) – ELT L 176, 27.6.2013.

[3] EBA/GL/2014/13

	sisestamise, säilitamise, töötlemise ja aruandluse, samuti järelevalve-, äri- ja otsustustoeteenused.
IKT käideldavuse ja talitluspidevusega seotud risk	Risk, et IKT-riistvara- või -tarkvarakomponendid võivad mõjutada negatiivselt IKT-süsteemide ja andmete toimivust ja kättesaadavust, sealhulgas põhjustada võimetuse õigeaegselt taastada krediidiasutuse või investeerimisühingu teenuseid; IKT-süsteemi halduse puudujäägid või muud asjaolud, mida on täpsustatud lisas.
IKT-turvarisk	Risk, mis on seotud volitamata juurdepääsuga IKT-süsteemidele ja andmetele krediidiasutuse või investeerimisühingu seest või väljastpoolt (näiteks küberründed), mida on täpsustatud lisas.
IKT-muutustega seotud risk	Risk, mis tuleneb krediidiasutuse või investeerimisühingu suutmatusest hallata IKT-süsteemi muutusi õigeaegselt ja kavakohaselt, eriti suuri ja keerukaid muutuskavasid, mida on täpsustatud lisas.
IKT andmetervikluse risk	Risk, et IKT-süsteemides säilitatavad ja töödeldavad andmed on mittetäielikud, ebatäpsed või eri süsteemides ebajärjekindlad, mis tuleneb näiteks IKT-kontrollide nõrkusest või puudumisest IKT-andmete elutsükli erinevates etappides (näiteks andmearhitektuuri projekteerimine, andmemudelite ja/või andmesõnastike loomine, sisendandmete verifitseerimine, andmete väljastamise, ülekande või töötlemise, sealhulgas visualiseeritavate väljundandmete kontrollimine) ning mis kahjustab krediidiasutuse või investeerimisühingu võimet pakkuda teenuseid või esitada (riski)juhtimis- või finantsandmeid õigesti ja õigeaegselt, nagu on täpsustatud lisas.
IKTga seotud tegevuse edasiandmise risk	Risk, et kolmanda isiku või kontserni teise üksuse osalemine (kontsernisisene tegevuse edasiandmine) IKT-süsteemide või seonduvate teenuste pakkumises mõjutab negatiivselt krediidiasutuse või investeerimisühingu tulemuslikkust ja riskijuhtimist, nagu on täpsustatud lisas.

3. Rakendamine

Kohaldamise alguskuupäev

9. Käesolevaid suuniseid kohaldatakse alates 1. jaanuarist 2018.

4. IKT-riskide hindamisele esitatavad nõuded

Jaotis 1. Üldsätted

10. Pädevad asutused peaksid hindama IKT-riski ning IKT valdkonna juhtimiskorraldust ja strateegiat SREPi protsessi osana, järgides EBA SREPi suuniste jaotises 2 kirjeldatud minimaalse sekkumise mudelit ja proportsionaalsuse kriteeriumeid. Eelkõige tähendab see järgmist:

    a. IKT-riski hindamise sagedus sõltub minimaalse sekkumise mudelist, mis lähtub krediidiasutusele või investeerimisühingule määratud SREPi kategooriast, ja selle konkreetsest järelevalvealase kontrolli programmist, ning

    b. IKT-hindamise põhjalikkus, üksikasjalikkus ja mahukus peaks olema vastavuses krediidiasutuse või investeerimisühingu suuruse, ülesehituse ja tegevuskeskkonnaga ning tema tegevuse laadi, ulatuse ja keerukusega.

11. Seoses krediidiasutuse või investeerimisühingu suhtes rakendatava järelevalvealase sekkumise ja dialoogi ulatuse, sageduse ja mahukusega ning standarditega, millele krediidiasutus või investeerimisühing peab järelevalve eelduste kohaselt vastama, kohaldatakse käesolevates suunistes läbivalt proportsionaalsuse põhimõtet.

12. Pädevad asutused võivad ajakohastatud hinnangu andmiseks kasutada ja arvesse võtta krediidiasutuse või investeerimisühingu või pädeva asutuse poolt teiste riskide või SREPi elementide hindamise käigus juba tehtud tööd. Nimelt peaksid pädevad asutused käesolevate suunistega ettenähtud hindamisi läbi viies valima asjakohaseima järelevalvealase lähenemisviisi ja metoodika, mis on asjaomase krediidiasutuse või investeerimisühingu jaoks sobivaim ja proportsionaalne, ning pädevad asutused peaksid kasutama oma hinnangu sisenditena olemasolevaid ja kättesaadavaid dokumente (näiteks asjakohased aruanded ja muud dokumendid, koosolekud (riski)juhtidega, kohapealsete kontrollide tulemused).

13. Pädevad asutused peaksid koondama käesolevates suunistes määratletud kriteeriumide hindamistulemused ning kasutama neid EBA SREPi suunistega ette nähtud SREPi elementide hindamise kohta järelduste tegemiseks.

14. Eriti käesolevate suuniste jaotise 2 kohaselt tehtav juhtimiskorralduse ja IKT-strateegia hindamine peaks andma tulemused, mis kajastuksid EBA SREPi suuniste jaotisega 5 ette nähtud juhtimiskorralduse ja kogu krediidiasutust või investeerimisühingut hõlmavate kontrollimeetmete elemendi hindamises ning vastavalt ka selle SREPi elemendi punktisummas. Lisaks peaksid pädevad asutused arvestama, et iga IKT-strateegia hinnangust tulenevat olulist negatiivset mõju

krediidiasutuse või investeerimisühingu äristrateegiale või mis tahes kahtlust, et krediidiasutus või investeerimisühing ei pruugi omada piisavalt IKT-ressursse ja -võimekust kavandatud oluliste strateegiliste muudatuste elluviimiseks ja toetuseks, tuleks arvestada ka EBA SREPi suuniste jaotise 4 kohases ärimudeli analüüsis.

15. Nende suuniste jaotises 3 osutatud IKT-riski hinnangu tulemust tuleks kajastada operatsiooniriski hinnangus ning seda tuleks arvestada ka EBA SREPi suuniste punktis 6.4 sätestatud asjakohases punktisummas.

16. Tuleb märkida, et kuigi üldiselt peaksid pädevad asutused hindama riskide allkategooriaid põhikategooriate osana (näiteks IKT-riski hinnatakse operatsiooniriski raames), võivad nad juhul, kui peavad allkategooriaid oluliseks, hinnata neid eraldi. Sellepärast esitatakse käesolevates suunistes juhuks, kui pädev asutus tuvastab IKT-riski olulise riskina, ka punktitabel (tabel 1), mida tuleks kasutada IKT-riskile kui eraldiseisvale allkategooriale punktide andmiseks lähtuvalt EBA SREPi suuniste üldisest lähenemisviisist kapitalile avalduvate riskide hindamisel.

17. Et teha kindlaks, kas IKT-riski tuleks käsitleda olulisena ja kas seetõttu tuleks seda hinnata ja anda sellele punkte operatsiooniriski allkategooriana, võivad pädevad asutused kasutada EBA SREPi suuniste punktis 6.1 määratletud kriteeriumeid.

18. Käesolevate suuniste kohaldamisel peaksid pädevad asutused vajaduse korral kaaluma lisas esitatud mitteammendavat IKT-riski allkategooriate ja riskistsenaariumide loetelu, võttes arvesse, et lisa keskendub IKT-riskidele, mis võivad põhjustada tõsist kahju. Pädevad asutused võivad jätta mõne klassifikatsioonis hõlmatud IKT-riski välja, kui see ei ole nende hinnangu järgi oluline. Krediidiasutuselt või investeerimisühingult eeldatakse pigem oma riskiklassifikatsiooni kui lisas esitatud IKT-riskide klassifikatsiooni kasutamist.

19. Juhul kui suuniseid kohaldatakse piiriülestele pangakontsernidele ja nende üksustele ning loodud on järelevalvekolleegium, peavad osalevad pädevad asutused SREPi suuniste punkti 11.1 kohasel järelevalvealasel läbivaatamisel ja hindamisel tehtava koostöö raames iga kontserni liikme puhul võimalikult suurel määral järjepidevalt koordineerima iga teabeühiku täpset ja üksikasjalikku ulatust.

Jaotis 2. Krediidiasutuste ja investeerimisühingute IKT valdkonna juhtimise ja strateegia hindamine

2.1 Üldpõhimõtted

20. Pädevad asutused peaksid hindama, kas krediidiasutuse või investeerimisühingu üldine juhtimis- ja sisekontrolliraamistik hõlmab nõuetekohaselt IKT-süsteeme ja seonduvaid riske ning kas juhtimisorgan käsitleb ja juhib neid aspekte piisavalt, sest IKT on krediidiasutuse või investeerimisühingu õige toimimise lahutamatu osa.

21. Hindamist läbi viies peaksid pädevad asutused võtma aluseks hea juhtimiskorralduse ja riskikontrollimeetmete nõuded ja standardid, mis on sätestatud EBA juhtimiskorralduse suunistes (GL 44)[4] ning selle valdkonna rahvusvahelistes suunistes niivõrd, kui need on IKT-süsteemide ja -riskide eripära arvestades kohaldatavad.

22. Käesoleva jaotise kohane hindamine ei hõlma IKT-süsteemi halduse, riskijuhtimise ja kontrollide konkreetseid elemente, mis keskenduvad suuniste jaotises 3 käsitletud erinevate IKT-riskide juhtimisele, vaid see keskendub järgmistele valdkondadele:

    a. IKT-strateegia – kas krediidiasutusel või investeerimisühingul on sobivalt hallatav ning tema äristrateegiaga kooskõlas olev IKT- strateegia;

    b. üldine juhtimiskorraldus – kas krediidiasutuse või investeerimisühingu üldine sisejuhtimiskord on krediidiasutuse või investeerimisühingu IKT-süsteemide osas piisav, ning

    c. IKT-risk krediidiasutuse või investeerimisühingu riskijuhtimisraamistikus – kas krediidiasutuse või investeerimisühingu riskijuhtimis- ja sisekontrolliraamistik kaitseb krediidiasutuse või investeerimisühingu IKT-süsteeme piisavalt hästi.

23. Kuigi punkti 22 alapunktis a antakse teavet krediidiasutuse või investeerimisühingu juhtimise kohta, peaks see peamiselt kajastuma EBA SREPi suuniste jaotises 4 käsitletud ärimudeli hindamises. Alapunktid b ja c täiendavad EBA SREPi suuniste jaotises 5 käsitletud teemade hindamist ning käesolevates suunistes kirjeldatud hinnangud peaksid kajastuma EBA SREPi suuniste jaotise 5 alusel tehtud vastavas hindamises.

24. Sellise riskihindamise tulemus peaks asjakohasel juhul kajastuma käesolevate suuniste jaotises 3 kirjeldatud riskijuhtimise ja kontrollimeetmete hindamises.

[4] EBA suunised juhtimiskorralduse kohta, GL 44, 27. september 2011.

2.2 IKT-strateegia

25. Käesoleva jaotise alusel peaksid pädevad asutused hindama, kas krediidiasutusel või investeerimisühingul on olemas selline IKT-strateegia, mille üles kohaldab krediidiasutuse või investeerimisühingu juhtorgan piisavat järelevalvet, mis on kooskõlas äristrateegiaga – eelkõige selleks, et hoida IKT ajakohasena ning kavandada või rakendada olulisi ja keerulisi muutusi IKT valdkonnas –, ning mis toetab krediidiasutuse või investeerimisühingu ärimudelit.

2.2.1 IKT-strateegia arendamine ja sobivus

26. Pädevad asutused peaksid hindama, kas krediidiasutus või investeerimisühing on IKT-strateegia ettevalmistamiseks ja arendamiseks kehtestanud oma IKTga seotud tegevuse laadi, ulatust ja keerukust arvestades proportsionaalse raamistiku. Hindamist läbi viies peaksid pädevad asutused arvestama, kas

    a. tegevussuunda(de) kõrgem juhtkond [5] osaleb krediidiasutuse või investeerimisühingu strateegiliste IKT-prioriteetide määratlemises piisavalt ning IKT-funktsiooni kõrgem juhtkond on omalt poolt teadlik peamiste äristrateegiate ja algatuste arendamisest, kavandamisest ja käivitamisest, et tagada IKT-süsteemide, IKT-teenuste ja IKT-funktsiooni (s.o nende süsteemide juhtimise ja rakendamise eest vastutava talituse) ja äristrateegia pidev kooskõlastamine, ning IKTd ajakohastatakse tõhusalt;

    b. IKT-strateegia on dokumenteeritud ning seda toetavad konkreetsed rakenduskavad, eriti seoses oluliste vahe-eesmärkide ja ressursside (sealhulgas rahaliste vahendite ja inimressursside) kavandamisega, et tagada nende realistlikkus ja võimaldada IKT-strateegia elluviimine;

    c. krediidiasutus või investeerimisühing ajakohastab regulaarselt oma IKT-strateegiat, eriti kui äristrateegia muutub, et tagada IKT ja äritegevuse keskmise pikkusega ja pikaajaliste eesmärkide, kavade ja tegevuste kooskõla, ning

    d. krediidiasutuse või investeerimisühingu juhtorgan kinnitab IKT-strateegia ja -rakenduskavad ning jälgib nende rakendamist.

2.2.2 IKT-strateegia rakendamine

27. Kui krediidiasutuse või investeerimisühingu IKT-strateegia nõuab oluliste ja keerukate IKT-süsteemi muutuste või selliste muutuste rakendamist, millel on oluline mõju krediidiasutuse või investeerimisühingu ärimudelile, peaksid pädevad asutused hindama, kas krediidiasutus või investeerimisühing on kehtestanud oma suuruse, IKTga seotud tegevuste ja muudatuste tasemega proportsionaalse kontrolliraamistiku, et toetada IKT-strateegia tõhusat rakendamist. Hindamist läbi viies peaksid pädevad asutused veenduma, kas kontrolliraamistik

[5] Kõrgem juhtkond ja juhtorgan, nagu need on määratletud 26. juuni 2013. aasta direktiivi 2013/36/EL artikli 3 punktis 7 (juhtorgan) ja artikli 3 punktis 9 (kõrgem juhtkond).

a. hõlmab juhtimisprotsesse (näiteks edusammude ja eelarve järelevalvet ja aruandlust) ning asjaomaseid organeid (näiteks projektijuhtimisbürood, IKT-juhtrühma või samaväärseid organeid), et toetada tõhusalt strateegiliste IKT-programmide rakendamist;

b. sisaldab strateegiliste IKT-programmide rakendamisega seotud ülesannete ja vastutusalade määratlusi ja jaotust, pöörates erilist tähelepanu oluliste ja keerukate IKT-muutuste korraldamise, juhtimise ja järelevalve peamiste osapoolte kogemusele ning organisatsioonile ja personalile avalduva laiaulatuslikuma mõju haldamisele (näiteks toimetulek muutustele vastuseisuga, koolitus, suhtlus);

c. kasutab sõltumatuid kontrolli- ja siseauditifunktsioone eesmärgiga tagada kindlus, et IKT-strateegia rakendamisega seotud riskid tuvastatakse, hinnatakse ja maandatakse tõhusalt ning et IKT-strateegia rakendamiseks kasutatav haldusraamistik on tõhus, ning

d. hõlmab planeerimise ja kavade läbivaatamise protsessi, mis tagab paindlikkuse reageerimisel tuvastatud olulistele probleemidele (näiteks kogetud rakendusprobleemid või viivitused) või välistele arengusuundumustele (näiteks olulised muutused ärikeskkonnas, tehnoloogilised probleemid või uuendused), et tagada strateegilise rakenduskava õigeaegne kohandamine.

2.3 Üldine juhtimiskorraldus

28. EBA SREPi suuniste jaotise 5 kohaselt peaksid pädevad asutused hindama, kas krediidiasutusel või investeerimisühingul on eesmärgile vastav asjakohane ja läbipaistev organisatsioonistruktuur ja kas ta on rakendanud asjakohase juhtimiskorra. Konkreetselt IKT-süsteeme silmas pidades ning kooskõlas EBA juhtimiskorralduse suunistega tuleks hinnata järgmist:

    a. krediidiasutusel või investeerimisühingul on usaldusväärne ja läbipaistev organisatsioonistruktuur, mis sisaldab selgelt IKTga seonduvaid vastutusalasid, sealhulgas juhtorgan ja selle komiteed, ning et IKT eest vastutavatel võtmeisikutel (näiteks infojuht, tegevjuht või samaväärne ametikoht) oleks piisav kaudne või otsene juurdepääs juhtorganile, et tagada oluliste IKTga seotud teabe ja probleemide edastamine, arutelu ja nende üle otsustamine juhtorgani tasandil, ning

    b. juhtorgan on IKT-riskidest teadlik ja ohjab neid.

29. Lisaks EBA SREPi suuniste punktile 5.2 peaksid pädevad asutused hindama, kas krediidiasutuse või investeerimisühingu IKTga seotud tegevuse edasiandmise põhimõtted ja strateegia võtavad vajaduse korral arvesse IKTga seotud tegevuse edasiandmise mõju krediidiasutuse või investeerimisühingu tegevusele ja ärimudelile.

2.4 IKT-risk krediidiasutuse või investeerimisühingu riskijuhtimisraamistikus

30. Hinnates kogu krediidiasutust või investeerimisühingut hõlmavaid riskijuhtimis- ja sisekontrollimeetmeid, nagu näeb ette EBA SREPi suuniste jaotis 5, peaksid pädevad asutused kaaluma, kas krediidiasutuse või investeerimisühingu riskijuhtimis- ja sisekontrolliraamistik kaitseb piisavalt krediidiasutuse või investeerimisühingu IKT-süsteeme viisil, mis on asutuse suuruse ja

tegevuste ning IKT-riskiprofiiliga proportsionaalne, nagu määratletud jaotises 3. Eelkõige peaksid pädevad asutused tegema kindlaks, kas

a. riskivalmidus ning sisemise kapitali adekvaatsuse hindamise protsess võtavad üldise riskistrateegia ning sisemise kapitali määratlemisel laiema operatsiooniriski kategooria raames arvesse IKT-riske, ning kas

b. IKT-riskid kuuluvad kogu krediidiasutust või investeerimisühingut hõlmava riskijuhtimis- ja sisekontrolliraamistiku kohaldamisalasse.

31. Pädevad asutused peaksid võtma punkti a kohasel hindamisel arvesse nii eeldatavaid kui ka negatiivseid stsenaariume, näiteks krediidiasutuse- või investeerimisühingupõhises või järelevalvealases stressitestis sisalduvaid stsenaariumid.

32. Seoses punktiga b peaksid pädevad asutused hindama, kas EBA SREPi suuniste punkti 104 alapunktides a ja d ning punkti 105 alapunktides a ja c kirjeldatud sõltumatud kontrolli- ja siseauditifunktsioonid on sobivad, et tagada IKT ning kontrolli- ja siseauditifunktsioonide vaheline piisav sõltumatus, arvestades krediidiasutuse või investeerimisühingu suurust ja IKT-riskiprofiili.

2.5 Järelduste kokkuvõte

33. Kõnealused tulemused peaksid kajastuma EBA SREPi suuniste jaotise 5 kohases järelduste kokkuvõttes ning moodustama osa vastavast punktisummast kooskõlas EBA SREPi suuniste tabelis 3 esitatud kaalutlustega.

34. IKT-strateegia hindamisel tuleks järeldusi tehes kaaluda järgmisi punkte:

a. kui pädevad asutused järeldavad, et krediidiasutuse või investeerimisühingu juhtimisraamistik on krediidiasutuse või investeerimisühingu IKT-strateegia arendamiseks ja rakendamiseks punkti 2.2 kohaselt ebapiisav, peaks see kajastuma krediidiasutuse või investeerimisühingu juhtimiskorralduse hinnangus vastavalt EBA SREPi suuniste jaotise 5 punkti 87 alapunktile a;

b. kui pädevad asutused järeldavad eelkirjeldatud punkti 2.2 kohastes hinnangutes, et IKT-strateegia ja äristrateegia vahel tekiks oluline lahknevus, millel võib olla oluline negatiivne mõju krediidiasutuse või investeerimisühingu pikaajalistele äri- ja/või finantseesmärkidele, jätkusuutlikkusele ja/või ärimudelile või tegevusvaldkondadele või -suundadele, mis on EBA SREPi suuniste punkti 62 alapunkti a järgi kõige olulisemad, peaks see kajastuma SREPi suuniste jaotise 4 punkti 70 alapunktide b ja c kohases ärimudeli hindamises, ning

c. kui pädevad asutused järeldavad eelkirjeldatud punkti 2.2 kohastes hinnangutes, et krediidiasutusel või investeerimisühingul ei pruugi olla piisavalt IKT-ressursse ega IKT-rakendamissuutlikkust, et viia ellu ja toetada kavandatud strateegilisi muutusi, peaks see kajastuma EBA SREPi suuniste jaotise 4 punkti 70 alapunkti b kohases ärimudeli hindamises.

Jaotis 3. Krediidiasutuse või investeerimisühingu IKT-riskide suuruse ja kontrollimeetmete hindamine

3.1 Üldised kaalutlused

35. Pädevad asutused peaksid hindama, kas krediidiasutus või investeerimisühing on oma IKT-riske nõuetekohaselt tuvastanud, hinnanud ja maandanud. See protsess peaks olema osa operatsiooniriski juhtimise raamistikust ja kooskõlas operatsiooniriski hindamisel kasutatava lähenemisviisiga.

36. Kõigepealt peaksid pädevad asutused tegema kindlaks krediidiasutusele või investeerimisühingule avalduvad või avalduda võivad olulised olemuslikud IKT-riskid, millele järgneb krediidiasutuse või investeerimisühingu IKT-riskide juhtimise raamistiku ning nende maandamise menetluste ja meetmete tõhususe hindamine. Hindamise tulemus peaks kajastuma järelduste kokkuvõttes, mida arvestatakse SREPi suuniste operatsiooniriski punktisummas. Kui IKT-riski peetakse oluliseks ning pädev asutus soovib määrata individuaalse punktisumma, tuleks kasutada tabelit 1, et anda sellele riskile punktid operatsiooniriski allkategooriana.

37. Käesoleva jaotise kohasel riskihindamisel peaksid pädevad asutused kasutama järelevalvealase hindamise prioriteetide kindlaksmääramisel kõiki EBA SREPi suuniste jaotise 6 punktis 127 nimetatud kättesaadavaid andmeallikaid, näiteks krediidiasutuse või investeerimisühingu riskijuhtimistegevusi, aruandeid ja tulemusi. Samuti peaksid pädevad asutused kasutama selleks hindamiseks teisi andmeallikaid, sealhulgas järgmisi, kui asjakohased:

    a. IKT-riskide ja -kontrollimeetmete enesehinnangud (kui need on sisemise kapitali adekvaatsuse hindamise protsessi teabes esitatud);
    b. krediidiasutuse või investeerimisühingu juhtorganile esitatud IKT-riskiga seotud juhtimisteave, näiteks regulaarsed või intsidentidest ajendatud IKT-riski aruanded (sealhulgas tegevuskahjude andmebaasist), IKT-riskile avatuse andmed krediidiasutuse või investeerimisühingu riskijuhtimisfunktsioonilt;
    c. krediidiasutuse või investeerimisühingu auditikomiteele teatatud IKTga seotud sise- ja välisauditite tulemused.

3.2 Oluliste IKT-riskide tuvastamine

38. Pädevad asutused peaksid tuvastama krediidiasutusele või investeerimisühingule avalduvaid või avalduda võivaid olulisi IKT-riske allpool kirjeldatud tegevuste kaudu.

3.2.1 Krediidiasutuse või investeerimisühingu IKT-riskiprofiili läbivaatamine

39. Krediidiasutuse või investeerimisühingu IKT-riskiprofiili läbi vaadates peaksid pädevad asutused kaaluma kogu asjakohast teavet krediidiasutuse või investeerimisühingu IKT-riskile avatuse kohta, sealhulgas punkti 37 kohast teavet ning tuvastatud olulisi puudujääke või lünki käesolevate suuniste jaotises 2 käsitletud IKT-korralduses ja kogu krediidiasutust või investeerimisühingut hõlmavates kontrollimeetmetes, ning vaatama vajadusel selle teabe proportsionaalselt läbi. Kõnealuse läbivaatamise käigus peaksid pädevad asutused arvestama järgmist:
    a. krediidiasutuse või investeerimisühingu IKT-süsteemide olulise häire võimalik mõju riigisisesele või rahvusvahelisele finantssüsteemile;
    b. kas krediidiasutust või investeerimisühingut võivad mõjutada IKT-turvariskid või IKT käideldavuse ja talitluspidevusega seotud riskid, mis tulenevad sõltuvusest internetist või uuenduslike IKT-lahenduste või teiste selliste turustuskanalite laialdasest kasutuselevõtust, mis võivad muuta krediidiasutuse või investeerimisühingu tõenäolisemaks küberründe sihtmärgiks;
    c. kas krediidiasutus või investeerimisühing võib olla IKT-turvariskide, IKT käideldavuse ja talitluspidevusega seotud riskide, IKT andmetervikluse riskide või IKT-muutustega seotud riskide suhtes avatum oma IKT-süsteemide keeruka (näiteks ühinemiste ja ülevõtmiste tulemusel) või vananenud olemuse tõttu;
    d. kas krediidiasutus või investeerimisühing rakendab oma IKT-süsteemides ja/või IKT-funktsioonis olulisi muudatusi (näiteks ühinemiste, ülevõtmiste, loovutamiste või IKT-põhisüsteemide väljavahetamise tulemusel), mis võivad mõjutada negatiivselt IKT-süsteemide stabiilsust või korrapärast toimimist ning võivad tekitada olulisi IKT käideldavuse ja talitluspidevusega seotud riske, IKT-turvariske, IKT-muutustega seotud riske või IKT andmetervikluse riske;
    e. kas krediidiasutus või investeerimisühing on kontsernisiseselt või -väliselt edasi andnud IKT-teenuseid või -süsteeme, mis võivad muuta ta avatuks olulistele IKTga seotud tegevuse edasiandmise riskidele;
    f. kas krediidiasutus või investeerimisühing rakendab jõuliselt IKT-kulude kokkuhoiumeetmeid, mis võivad põhjustada vajalike IKT-investeeringute, ressursside ja oskusteabe vähenemist ja suurendada avatust kõigile klassifikatsioonis esindatud IKT-riski liikidele;
    g. kas oluliste IKT-toimingute/andmekeskuste asukoht (näiteks piirkonnad või riigid) võib muuta krediidiasutuse või investeerimisühingu avatuks loodusõnnetuste (näiteks üleujutuste või maavärinate), poliitilise ebastabiilsuse või tööjõukonfliktide ja rahvarahutuste suhtes, põhjustades olulisi IKT käideldavuse ja talitluspidevusega seotud riske ning IKT-turvariske.

3.2.2 Oluliste IKT-süsteemide ja -teenuste läbivaatamine

40. Krediidiasutuse või investeerimisühingu usaldatavusele potentsiaalselt olulist mõju avaldavate IKT-riskide tuvastamise protsessi käigus peaksid pädevad asutused vaatama läbi krediidiasutuse või investeerimisühingu esitatud dokumendid ning kujundama arvamuse selle kohta, mis IKT-süsteemid ja -teenused on põhitegevuste korraliku toimimise, käideldavuse, talitluspidevuse ja turvalisuse seisukohast olulised.

41. Selleks peaksid pädevad asutused vaatama läbi meetodid ja protsessid, mille alusel krediidiasutus või investeerimisühing määratleb olulisi IKT-süsteeme ja -teenuseid, võttes arvesse, et viimane võib pidada teatud IKT-süsteemi ja -teenust oluliseks äritegevuse talitluspidevuse ja käideldavuse, turvalisuse (näiteks pettuste vältimise) ja/või konfidentsiaalsuse (näiteks andmekonfidentsiaalsuse) seisukohast. Läbivaatamise käigus peaksid pädevad asutused arvestama, et olulised IKT-süsteemid ja -teenused peaksid vastama vähemalt ühele järgmistest tingimustest:

    a. need toetavad krediidiasutuse või investeerimisühingu peamisi äritoiminguid ja turustuskanaleid (näiteks sularahaautomaadid, interneti- ja mobiilipangandus);

    b. need toetavad olulisimaid juhtimisprotsesse ja korporatiivseid funktsioone, sealhulgas riskijuhtimist (näiteks riskijuhtimis- ja rahahaldussüsteemid);

    c. neile kehtivad õiguslikud või regulatiivsed erinõuded (olemasolu korral), millest tulenevad mõne süsteemselt olulise teenuse (kui kohaldatav) parema käideldavuse, vastupidavuse, konfidentsiaalsuse või turvalisuse nõuded (näiteks andmekaitse õigusaktid või võimalik taaste sihtkestus (RTO) ehk maksimaalne aeg, mille järel peab süsteem või protsess olema pärast intsidenti taastatud, ja taaste sihtseis (RPO) ehk maksimaalne aeg, mille vältel võivad andmed pärast intsidenti kadunud olla);

    d. need töötlevad või säilitavad konfidentsiaalseid või tundlikke andmeid, millele volitamata juurdepääs võib mõjutada oluliselt krediidiasutuse või investeerimisühingu mainet, finantstulemusi või tema tegevuse usaldatavust ja talitluspidevust (näiteks tundlike kliendiandmetega andmebaasid), ja/või

    e. need pakuvad baasfunktsioone, mis on krediidiasutuse või investeerimisühingu nõuetekohaseks toimimiseks hädavajalikud (näiteks telekommunikatsiooni- ja ühenduvusteenused, IKT- ja küberturbeteenused).

3.2.3 Olulistele IKT-süsteemidele ja -teenustele avalduvate oluliste IKT-riskide tuvastamine

42. Arvestades eelkirjeldatud krediidiasutuse või investeerimisühingu IKT-riskiprofiili ning oluliste IKT-süsteemide ja -teenuste läbivaatamist, peaksid pädevad asutused kujundama arvamuse olulistest IKT-riskidest, mis võivad nende järelevalvealase hinnangu kohaselt märkimisväärselt mõjutada krediidiasutuste või investeerimisühingu IKT-süsteemide ja -teenuste usaldusväärsust.

43. Hinnates IKT-riskide võimalikku mõju krediidiasutuse või investeerimisühingu olulistele IKT-süsteemidele ja -teenustele, peaksid pädevad asutused võtma arvesse järgmist:

    a. rahaline mõju, sealhulgas (kuid mitte ainult) rahaliste ja muude varade kaotus, võimalikud hüvitised klientidele, õiguskaitse- ja hüvituskulud, lepingutest tulenevad kahjud, kaotatud tulu;

    b. äritegevuse katkemise võimalus, võttes arvesse mõjutatava finantsteenuse olulisust (kuid mitte ainult); klientide ja/või filiaalide ja töötajate arv, keda see võib mõjutada;

    c. võimalik mõju krediidiasutuse või investeerimisühingu mainele, võttes arvesse mõjutatava pangateenuse või operatiivtegevuse olulisust (näiteks kliendiandmete vargus); mõjutatavate IKT-süsteemide ja -teenuste väline profiil / nähtavus (näiteks mobiili- ja internetipangasüsteemid, müügikoht, sularahaautomaadid või maksesüsteemid);

d. regulatiivne mõju, sealhulgas võimalik avalik umbusaldus reguleerimisasutuse poolt, trahvid või isegi tegevuslubade muutmine;

e. strateegiline mõju krediidiasutusele või investeerimisühingule, näiteks strateegilise tähtsusega toote või äriplaanide kahjustamise või varguse korral.

44. Seejärel peaksid pädevad asutused jaotama tuvastatud oluliseks peetavad IKT-riskid järgmistesse IKT-riskide kategooriatesse, mille täiendavad kirjeldused ja näited on toodud lisas. Pädevad asutused peaksid kaaluma lisas esitatud IKT-riske jaotise 3 kohase hindamise käigus:

a. IKT käideldavuse ja talitluspidevusega seotud risk
b. IKT-turvarisk
c. IKT-muutustega seotud risk
d. IKT andmetervikluse risk
e. IKTga seotud tegevuse edasiandmise risk

Selle jaotuse eesmärk on aidata pädevatel asutusel kindlaks teha, mis riske (olemasolu korral) tuleks pidada oluliseks ning seetõttu järgmistes hindamisetappides hoolikamalt ja/või põhjalikumalt läbi vaadata.

3.3 Oluliste IKT-riskide maandamiseks kasutatavate kontrollimeetmete hindamine

45. Krediidiasutuse või investeerimisühingu IKT-jääkriski hindamiseks peaksid pädevad asutused vaatama läbi, kuidas krediidiasutus või investeerimisühing tuvastab, jälgib, hindab ja maandab pädeva asutuse poolt eelkirjeldatud hindamise käigus tuvastatud olulisi riske.

46. Selleks peaksid pädevad asutused seoses tuvastatud oluliste IKT-riskidega vaatama läbi

c. kehtivad IKT-riskide juhtimise põhimõtted, protsessid ja riskide vastuvõetavuse piirmäärad;

d. organisatsiooni juhtimise ja järelevalve raamistiku;

e. siseauditi hõlmavuse ja selle järeldused ning

f. kohaldatavad IKT-riskide kontrollimeetmed, mis on seotud tuvastatud oluliste IKT-riskidega.

47. Hindamisel tuleks arvesse võtta EBA SREPi suuniste jaotises 5 osutatud üldise riskijuhtimis- ja sisekontrolliraamistiku analüüsi tulemusi ning käesolevate suuniste jaotises 2 käsitletud krediidiasutuse või investeerimisühingu juhtimiskorraldust ja strateegiat, sest nimetatud valdkondades leitud olulised puudujäägid võivad mõjutada krediidiasutuse või investeerimisühingu võimet hallata ja maandada avatust IKT-riskidele. Asjakohasel juhul peaksid pädevad asutused kasutama ka käesolevate suuniste punktis 37 nimetatud andmeallikaid.

48. Pädevad asutused peaksid allpool esitatud hindamisetapid läbi viima viisil, mis on krediidiasutuse või investeerimisühingu tegevuse laadi, ulatuse ja keerukusega proportsionaalne, ning teostama krediidiasutuse või investeerimisühingu IKT-riskiprofiilile vastava järelevalvealase läbivaatamise.

3.3.1 IKT-riskide juhtimise põhimõtted, protsessid ja vastuvõetavuse piirmäärad

49. Pädevad asutused peaksid uurima, kas krediidiasutus või investeerimisühing on kehtestanud tuvastatud oluliste IKT-riskide suhtes asjakohased riskijuhtimise põhimõtted, protsessid ja vastuvõetavuse piirmäärad. See võib olla osa operatsiooniriski juhtimise raamistikust või eraldi dokument. Hindamisel peaksid pädevad asutused arvestama järgmist:

    a. riskijuhtimise põhimõtted on koostanud ja heaks kiitnud juhtorgan ja need sisaldavad piisavaid suuniseid krediidiasutuse või investeerimisühingu riskivalmiduse kohta ning peamisi kavandatavaid IKT-riski juhtimise eesmärke ja/või kohaldatavaid IKT-riski vastuvõetavuse piirmäärasid; asjaomased IKT-riski juhtimise põhimõtted peaksid olema edastatud ka kõigile asjaomastele sidusrühmadele;

    b. kohaldatavad põhimõtted hõlmavad kõiki tuvastatud oluliste IKT-riskide juhtimiseks olulisi elemente;

    c. krediidiasutus või investeerimisühing on rakendanud protsessi ja selle alusmenetlused seonduvate oluliste IKT-riskide tuvastamiseks (näiteks riskikontrolli enesehinnangud, riskistsenaariumide analüüsid) ja jälgimiseks ning

    d. krediidiasutus või investeerimisühing on kehtestanud IKT-riski juhtimise aruandluse, mis tagab kõrgema juhtkonna ja juhtorgani õigeaegse teavitamise ning võimaldab kõrgemal juhtkonnal ja/või juhtorganil hinnata ja jälgida, kas krediidiasutuse või investeerimisühingu IKT-riski maandamiskavad ja -meetmed on kooskõlas heakskiidetud riskivalmiduse ja/või vastuvõetavuse piirmääradega (olemasolu korral), ning jälgida oluliste IKT-riskide muutumist.

3.3.2 Organisatsiooni juhtimise ja järelevalve raamistik

50. Pädevad asutused peaksid hindama, kuidas kehtivad riskijuhtimise ülesanded ja vastutusalad on integreeritud organisatsiooni juhtimiskorraldusega, et tagada tuvastatud IKT-riskide juhtimine ja järelevalve. Seoses sellega peaksid pädevad asutused hindama, kas krediidiasutuse või investeerimisühingu puhul kehtib järgmine:

    a. selged ülesanded ja vastutusalad seonduva olulise IKT-riski tuvastamiseks, hindamiseks, jälgimiseks, maandamiseks, aruandluseks ja järelevalveks;

    b. riskidega seotud vastutusalad ja ülesanded on kõigile organisatsiooni asjaomastele üksustele (näiteks tegevussuunad, IT) ja protsessidele selgelt teatatud ja jaotatud ning nendega integreeritud, sealhulgas riskiteabe kogumise ja koondamise ning kõrgemale juhtkonnale ja/või juhtorganile edastamise ülesanded ja vastutusalad;

    c. IKT-riski juhtimise tegevusi teostatakse piisava hulga kvalifitseeritud töötajate ning sobivate tehniliste vahendite abil; kohaldatavate riskimaanduskavade usaldusväärsuse hindamiseks peaksid pädevad asutused hindama ka seda, kas krediidiasutus või investeerimisühing on eraldanud nende rakendamiseks piisavalt rahalisi vahendeid ja/või muid vajalikke ressursse;

    d. piisavad järelmeetmed ja asjakohane reaktsioon juhtorgani poolt, kui sõltumatud kontrollifunktsioonid avastavad seoses IKT-riski(de)ga midagi olulist, võttes arvesse mõne aspekti võimalikku delegeerimist komiteele (kui see on olemas), ning

e. kehtivate IKT-eeskirjade ja -põhimõtete erandid pannakse kirja ja nende suhtes rakendatakse sõltumatu kontrollifunktsiooni poolset dokumenteerivat läbivaatamist ja aruandlust, mis keskendub seotud riskidele.

3.3.3 Siseauditi hõlmavus ja järeldused

51. Pädevad asutused peaksid kaaluma, kas siseauditi funktsioon on kehtiva IKT-riski kontrolliraamistiku auditeerimise seisukohast tõhus, hinnates, kas

    a. IKT-riski kontrolliraamistikku auditeeritakse vajaliku kvaliteedi, põhjalikkuse ja sagedusega ning proportsionaalselt krediidiasutuse või investeerimisühingu suuruse, tegevuste ja IKT-riskiprofiiliga;

    b. auditikava sisaldab krediidiasutuse või investeerimisühingu tuvastatud oluliste IKT-riskide auditeerimist;

    c. IKT-auditi olulised järeldused, sealhulgas kokkulepitud tegevused, teatatakse juhtorganile ning

    d. IKT-auditi järelduste, sealhulgas kokkulepitud tegevuste osas rakendatakse järelmeetmeid ning kõrgem juhtkond ja/või auditikomitee vaatab eduaruandeid regulaarselt läbi.

3.3.4 Tuvastatud oluliste IKT-riskidega seonduvad konkreetsed IKT-riskide kontrollimeetmed

52. Tuvastatud oluliste IKT-riskidega seoses peaksid pädevad asutused hindama, kas krediidiasutus või investeerimisühing on kehtestanud konkreetsed kontrollimeetmed nende riskide juhtimiseks. Allpool punktides on esitatud mitteammendav loetelu konkreetsetest kontrollimeetmetest, mida võiks kaaluda, hinnates punkti 3.2.3 alusel tuvastatud ja järgmistesse IKT-riski kategooriatesse liigitatud olulisi riske:

a. IKT käideldavuse ja talitluspidevusega seotud riskid;
b. IKT-turvariskid;
c. IKT-muutustega seotud riskid;
d. IKT andmetervikluse riskid;
e. IKTga seotud tegevuse edasiandmise riskid.

(a) Oluliste IKT käideldavuse ja talitluspidevusega seotud riskide juhtimise kontrollimeetmed

53. Lisaks EBA SREPi suuniste nõuetele (punktid 279–281) peaksid pädevad asutused hindama, kas krediidiasutusel või investeerimisühingul on kasutusel sobiv raamistik IKT käideldavuse ja talitluspidevusega seotud riskide tuvastamiseks, mõistmiseks, mõõtmiseks ja maandamiseks.

54. Hindamisel peaksid pädevad asutused eelkõige arvestama järgmist:

a. kas raamistikus on määratletud olulised IKT-protsessid ja asjakohased IKT-tugisüsteemid, mis peaksid olema osa vastupidavuse ja talitluspidevuse kavadest, mis sisaldavad järgmist:

    i. oluliste äriprotsesside ja tugisüsteemide sõltuvusseoste põhjalik analüüs;

ii. IKT-tugisüsteemide taaste-eesmärkide kindlaksmääramine (mis tavaliselt määratakse kindlaks ettevõtte poolt ja/või eeskirjade alusel taaste sihtkestuse (RTO) või taaste sihtseisu (RPO) eesmärgina);

iii. asjakohane hädaolukorrakava, mis võimaldab oluliste IKT-süsteemide ja teenuste käideldavust, talitluspidevust ja taastamist, et vähendada lubatud piirides krediidiasutuse või investeerimisühingu toimimise häireid;

b. kas raamistikku kuuluvad vastupidavuse ja talitluspidevuse kontrollikeskkonna põhimõtted ja standardid ning tegevuskontrollid, mis hõlmavad järgmist:

i. meetmed, mis aitavad vältida seda, et üksik stsenaarium, intsident või avarii mõjutaks korraga nii IKT tootmis- kui ka taastamise süsteeme;

ii. IKT-süsteemi varundamis- ja taasteprotseduurid olulise tarkvara ja andmete jaoks, mis tagavad, et varukoopiad salvestatakse turvalises ja piisavalt kauges asukohas, nii et ükski intsident ega avarii ei saaks neid olulisi andmeid hävitada ega rikkuda;

iii. seirelahendused IKT käideldavuse ja talitluspidevusega seotud intsidentide õigeaegseks avastamiseks;

iv. intsidentide dokumenteeritud halduse ja eskalatsiooniprotsess, mis annab juhiseid ka erinevate intsidentide halduse ja eskaleerumisega seotud ülesannete ja vastutusalade kohta, samuti kriisikomitee(de) liikmete ning hädaolukorras rakendatava käsuahela kohta;

v. füüsilised meetmed nii krediidiasutuse või investeerimisühingu olulise IKT-taristu (näiteks andmekeskuste) kaitseks keskkonnariskide (näiteks üleujutuste ja teiste loodusõnnetuste) eest kui ka IKT-süsteemide jaoks sobiva töökeskkonna tagamiseks (näiteks kliimaseade);

vi. protsessid, ülesanded ja vastutusalad, mis tagavad, et ka tellitud IKT-süsteemid ja -teenused on piisavate vastupidavuse ja talitluspidevuse lahenduste ja kavadega kaetud;

vii. oluliste IKT-süsteemide ja -teenuste jaoks IKT toimivuse ja võimsuse kavandamise ja seire lahendused, millel on kindlaks määratletud käideldavusnõuded, et avastada õigeaegselt olulised toimivuse ja võimsuse piirangud;

viii. kui vajalik ja asjakohane, lahendused oluliste internetitegevuste või -teenuste (näiteks elektroonilise panganduse) kaitseks teenusetõkestamise ründe ning teiste küberrünnete vastu internetist, mille eesmärk on vältida või häirida kõnealuste tegevuste ja teenuste käideldavust;

c. kas raamistik testib IKT käideldavuse ja talitluspidevuse lahendusi mitmesuguste realistlike stsenaariumide korral, sealhulgas küberründed, tõrkesiirde testid ning kriitilise tähtsusega tarkvara ja andmete varukoopiate testid,

i. mis on kavandatud, sõnastatud ja dokumenteeritud ning mille tulemusi kasutatakse IKT käideldavuse ja talitluspidevuse lahenduste tõhususe parandamiseks;

ii. mis hõlmavad organisatsioonisiseseid sidusrühmi ja funktsioone, näiteks tegevussuundade juhte, sealhulgas talitluspidevuse, intsidentidele ja kriisidele reageerimise meeskondi ja asjaomaseid organisatsioonivälised sidusrühmi, ning

iii. millesse kaasatakse asjakohaselt juhtorgan ja kõrgem juhtkond (näiteks kriisihaldusmeeskondade liikmetena), keda teavitatakse ka testide tulemustest.

(b) Oluliste IKT-turvariskide juhtimise kontrollimeetmed

55. Pädevad asutused peaksid hindama, kas krediidiasutusel või investeerimisühingul on kasutusel tõhus raamistik IKT-turvariski tuvastamiseks, mõistmiseks, mõõtmiseks ja maandamiseks. Hindamisel peaksid pädevad asutused eelkõige uurima, kas raamistik hõlmab järgmist:

a. selgelt määratletud ülesanded ja vastutusalad seoses järgmisega:
   i. isiku(d) ja/või komitee(d), kes vastutavad ja/või on aruandekohustuslikud IKT turvalisuse igapäevahalduse ning üldiste IKT turvalisuse põhimõtete järgimise vallas, pöörates tähelepanu nende sõltumatusele;
   ii. IKT-turvakontrollide kavandamine, rakendamine, haldamine ja järelevalve;
   iii. oluliste IKT-süsteemide ja -teenuste kaitse näiteks haavatavuse hindamise protsessi, tarkvara turvaaukude haldamise, lõpp-punkti kaitse (näiteks pahavara viiruse vastu), sissetungide avastamise ja vältimise vahendite kasutuselevõtu kaudu;
   iv. asutuseväliste ja -siseste IKT turvaintsidentide vältimine, klassifitseerimine ja käsitlemine, sealhulgas intsidentidele reageerimine ning IKT-süsteemide ja -teenuste jätkamine ja taastamine;
   v. regulaarsed ja ennetavad ohuhinnangud asjakohaste turvakontrollide haldamiseks;

b. IKT turvapõhimõtted, mis võtavad arvesse ja vajaduse korral järgivad rahvusvaheliselt tunnustatud IKT turvastandardeid ja -põhimõtteid (näiteks minimaalõiguste printsiip ehk juurdepääsuõiguse piiramine minimaalsele tasemele, mis võimaldab normaalset toimimist, ja süvakaitse põhimõte ehk süsteemi kui terviku turvalisust suurendavate mitmekordsete turvamehhanismide projekteerimine süsteemi arhitektuuri);

c. võimalikku pettuseriski ja/või konfidentsiaalsete andmete võimalikku väärkasutust ja/või kuritarvitamist kajastav IKT-süsteemide, -teenuste ja proportsionaalsete turvanõuete tuvastamise protsess koos tuvastatud IKT-süsteemide, -teenuste ja andmete korral kehtivate dokumenteeritud turvatingimustega, mis on kooskõlas krediidiasutuse või investeerimisühingu riskivalmidusega ja mille nõuetekohase rakendamise üle tehakse järelevalvet;

d. dokumenteeritud turvaintsidentide halduse ja eskalatsiooni protsess, mis annab juhiseid erinevate intsidentide halduse ja eskaleerumisega seotud ülesannete ja vastutusalade kohta, samuti kriisikomitee(de) liikmete ning turvalisusega seotud hädaolukorras rakendatava käsuahela kohta;

e. kasutus- ja haldustoimingute logimine, mis võimaldab tõhusat järelevalvet ning volitamata tegevuse õigeaegset avastamist ja sellele reageerimist, et aidata ja viia läbi turvaintsidentide kriminaaluurimised. Krediidiasutusel või investeerimisühingul peaksid olema kehtestatud logimispõhimõtted, milles on määratletud sobivad logide liigid ja logide säilitamise aeg;

f. teadlikkuse tõstmise kampaaniad või algatused, mille käigus tutvustatakse krediidiasutuse või investeerimisühingu kõigile tasanditele IKT-süsteemide ohutut kasutamist ja kaitset ning peamisi IKT turva- vm riske, millest nad peaksid teadlikud olema, eriti olemasolevad ja tekkivad küberohud (näiteks arvutiviirused, võimalikud organisatsioonisisesed või -välised kuritarvitused või ründed, küberründed), ning nende roll turvarikkumiste riski maandamisel;

g. piisavad füüsilised kaitsemeetmed (nt videovalve, sissetungihäire, turvauksed), et hoida ära volitamata füüsiline juurdepääs olulistele ja tundlikele IKT-süsteemidele (nt andmekeskustele);

h. meetmed IKT-süsteemide kaitseks rünnete eest, mis tulevad internetist (näiteks küberründed) või teistest välisvõrkudest (näiteks traditsioonilistest telekommunikatsioonivõrkudest või usaldusväärsete partneritega loodud ühendustest). Pädevad asutused peaksid uurima, kas krediidiasutuse või investeerimisühingu raamistik hõlmab järgmist:

   i. täieliku ja ajakohastatud andmeinventuuri haldamise protsess ja lahendused ning kõigi väljapoole suunatud võrguühenduste ülevaade (näiteks veebilehed, internetirakendused, juhtmeta internetiühendus, kaugjuurdepääs), mille kaudu kolmandad isikud võiksid organisatsioonisisestesse IKT-süsteemidesse tungida;

   ii. hoolikalt hallatavad ja jälgitavad turvameetmed (näiteks tulemüürid, puhverserverid, meilivahendusserverid, viirusetõrje ja sisuskannerid), mis kindlustavad sissetulevat ja väljaminevat võrguliiklust (näiteks e-post) ja väljapoole suunatud võrguühendusi, mille kaudu kolmandad isikud võiksid organisatsioonisisestesse IKT-süsteemidesse tungida;

   iii. protsessid ja lahendused, mis turvavad veebilehti ja rakendusi, mida võiks internetist ja/või väljastpoolt otse rünnata ning mis võiksid toimida organisatsioonisisestesse IKT-süsteemidesse sisenemise punktina. Üldiselt hõlmavad sellised protsessid ja lahendused tunnustatud turvasüsteemide arendustavade ning IKT-süsteemi tugevdamise ja haavatavuste skaneerimise tavade ühendamist ja/või täiendavate turvalahenduste, näiteks tulemüüride ja/või sissetungi avastamise ja/või sissetungi ärahoidmise süsteemide rakendamist;

   iv. regulaarne turvasüsteemide toimivuse testimine, et hinnata rakendatavate küberturbe- ja organisatsioonisiseste IKT-turvameetmete ja -protsesside tõhusust. Kõnealuseid teste peaksid tegema vajalike oskustega töötajad ja/või väliseksperdid, testide tulemused ja järeldused tuleks dokumenteerida ning edastada kõrgemale juhtkonnale ja/või juhtorganile. Kui see on vajalik ja asjakohane, peaks krediidiasutus või investeerimisühing saama nende testide abil teada, kas turvakontrolle ja - protsesse tuleks täiustada ja/või kinnitada täiendavalt nende tõhusust.

(c) Oluliste IKT-muutustega seotud riskide juhtimise kontrollimeetmed

56. Pädevad asutused peaksid hindama, kas krediidiasutusel või investeerimisühingul on IKT-muutustega seotud riskide tuvastamiseks, mõistmiseks, mõõtmiseks ja maandamiseks kehtestatud tõhus ning oma tegevuse laadi, ulatust ja keerukust ning IKT-riskiprofiili arvestades proportsionaalne raamistik. Krediidiasutuse või investeerimisühingu raamistik peaks hõlmama riske, mis seonduvad IKT-süsteemides tehtavate muutuste arenduse, testimise ja heakskiitmisega, sealhulgas tarkvara arendamise või muutmisega enne selle kasutuselevõttu tootmiskeskkonnas,

ning tagama IKT elutsükli piisava halduse. Hindamisel peaksid pädevad asutused eelkõige uurima, kas raamistik hõlmab järgmist:

a. dokumenteeritud protsessid muutuste haldamiseks ja kontrollimiseks IKT-süsteemides (näiteks seadistuse ja paikade haldamine) ning andmetes (näiteks veaparandused ja andmeparandused), mis tagavad IKT-riskide piisava juhtimise oluliste IKT-muutuste korral, mis võivad krediidiasutuse või investeerimisühingu riskiprofiili või riskide suurust oluliselt mõjutada;

b. tehnilised kirjeldused koos vajaliku ülesannete lahususega rakendatavate IKT-muutustega seotud protsesside eri etappides (näiteks lahenduste kavandamine ja arendamine, uue tarkvara ja/või muutuste testimine ja heakskiitmine, üle viimine ja juurutamine tootmiskeskkonda ning veaparandused), keskendudes rakendatavatele lahendustele ja ülesannete lahususele IKT tootmissüsteemides ja andmetes töötajate (nt arendajate, IKT-süsteemihaldurite, andmebaasihaldurite) või teiste osapoolte (näiteks äriklientide ja teenusepakkujate) tehtavate muutuste haldamisel ja kontrollimisel;

c. testimiskeskkonnad, mis kajastavad piisavalt hästi tootmiskeskkondi;

d. tootmiskeskkonnas ning testimis- ja arenduskeskkonnas olemasolevate rakenduste ja IKT-süsteemide inventuur, et vajalikke muutusi (näiteks versiooni ajakohastusi või täiustusi, süsteemide paikamist, seadistuste muutmist) oleks võimalik seonduvates IKT-süsteemides korralikult hallata, rakendada ja jälgida;

e. protsess, mis võimaldab kasutatavate IKT-süsteemide elutsüklit jälgida ja hallata, et tagada nende jätkuv vastavus tegelikele äri- ja riskijuhtimisvajadustele ning kindlustada kasutatavate IKT-lahenduste ja -süsteemide jätkuv toetamine nende pakkujate poolt; see protsess peab hõlmama asjakohast tarkvaraarenduse elutsükli protseduuri;

f. tarkvara lähtekoodi kontrollisüsteem ja asjakohased menetlused volitamata muutuste ärahoidmiseks organisatsioonisiseselt arendatava tarkvara lähtekoodis;

g. protsess, mille käigus kontrollitakse uute või oluliselt muudetud IKT-süsteemide ja tarkvara turvalisust ja haavatavust enne nende tootmiskeskkonnas kasutuselevõttu ja avamist võimalikele küberrünnetele;

h. protsess ja lahendused konfidentsiaalsete andmete volitamata või soovimatu avaldamise vältimiseks IKT-süsteemide asendamise, arhiveerimise, kasutuselt kõrvaldamise või hävitamise käigus;

i. sõltumatud läbivaatus- ja valideerimisprotsessid, et vähendada IKT-süsteemide muutuste rakendamisel inimvigade riski, mis võivad avaldada olulist negatiivset mõju krediidiasutuse või investeerimisühingu IKT käideldavusele, talitluspidevusele või turvalisusele (näiteks tulemüüri seadistuste olulised muutused) või krediidiasutuse või investeerimisühingu julgeolekule (näiteks tulemüüri muutused).

(d) Oluliste IKT andmetervikluse riskide juhtimise kontrollimeetmed

57. Pädevad asutused peaksid hindama, kas krediidiasutus või investeerimisühing on IKT andmetervikluse riskide tuvastamiseks, mõistmiseks, mõõtmiseks ja maandamiseks kehtestanud tõhusa ning oma tegevuse laadi, ulatust ja keerukust ning IKT-riskiprofiili arvestava

proportsionaalse raamistiku. Krediidiasutuse või investeerimisühingu raamistik peaks käsitlema riske, mis seonduvad IKT-süsteemides hoiustatavate ja töödeldavate andmete terviklikkuse kaitsega. Hindamisel peaksid pädevad asutused eelkõige arvestama, kas raamistik hõlmab järgmist:

g. põhimõtted, mis määratlevad andmete terviklikkuse haldamisega seotud ülesanded ja vastutusalad IKT-süsteemides (näiteks andmearhitekt, andmetöötlejad [6], andmekäitlejad [7], andmete omanikud/haldurid[8]) ning annavad juhiseid, mis andmed on andmetervikluse seisukohast olulised ja vajavad IKT-andmete elutsükli eri etappides konkreetseid IKT-kontrollimeetmeid (näiteks automaatsed sisendandmete valideerimise kontrollid, andmeedastuskontrollid, andmete kooskõlastus jne) või läbivaatamist (näiteks andmearhitektuuriga ühilduvuse kontroll);

h. dokumenteeritud andmearhitektuur, andmemudel ja/või andmesõnastik, mida valideeritakse asjaomaste äri- ja IT-sidusrühmadega, et toetada vajalikku andmete kooskõlastatust erinevates IKT-süsteemides ning tagada, et andmearhitektuur, andmemudel ja/või andmesõnastik oleks(id) kooskõlas äri- ja riskijuhtimisvajadustega;

i. lõppkasutajapoolse andmetöötluse lubamise ja selle kasutamise põhimõtted, eriti mis puudutab oluliste lõppkasutajapoolse andmetöötluse lahenduste määratlemist, registreerimist ja dokumenteerimist (näiteks oluliste andmete töötlemisel) ning eeldatavaid turvatasemeid, et hoida ära volituseta muutusi nii vahendis endas kui ka selles talletatavates andmetes;

j. dokumenteeritud erandite menetlemise protsess, et lahendada tuvastatud IKT andmetervikluse probleemid lähtuvalt nende olulisusest ja tundlikkusest.

58. Kui järelevalve alla kuuluva krediidiasutuse ja investeerimisühingu suhtes kohaldatakse Baseli pangajärelevalve komitee määruses 239 toodud riskiandmete tõhusa koondamise ja aruandluse põhimõtteid[9], peaksid pädevad asutused vaatama läbi krediidiasutuse või investeerimisühingu riskianalüüsi oma riskidest teatamise ja andmete koondamise võimekuse kohta, võrreldes seda asjaomaste kehtivate põhimõtete ja vastavate dokumentidega ning võttes arvesse põhimõtetes sisalduvat rakendamise ajakava ja üleminekukorda.

(e) Oluliste IKTga seotud tegevuse edasiandmise riskide juhtimise kontrollimeetmed

59. Pädevad asutused peaksid hindama, kas krediidiasutuse või investeerimisühingu tegevuse edasiandmise strateegia käsitleb kooskõlas Euroopa Pangandusjärelevalve Komitee tegevuse edasiandmise suunistega (2006) ja EBA SREPi suuniste punkti 85 alapunktis d esitatud nõudega IKTga seotud tegevuse edasiandmist, sealhulgas kontsernisisest tegevuse edasiandmist, millega pakutakse IKT-teenuseid kontserni piires. IKTga seotud tegevuse edasiandmise riske hinnates peaksid pädevad asutused võtma arvesse, et kõnealuseid riske saab käsitleda ka olemuslike

[6] Andmetöötleja vastutab andmete töötlemise ja kasutamise eest.

[7] Andmekäitleja vastutab andmete turvalise käitlemise, edastamise ja talletamise eest.

[8] Andmehaldur vastutab andmeelementide (nii sisu kui ka metaandmete) halduse ja kvaliteedi eest.

[9] Baseli pangajärelevalve komitee, riskiandmete tõhusa koondamise ja aruandluse põhimõtted, jaanuar 2013, kättesaadav internetis aadressil http://www.bis.org/publ/bcbs239.pdf.

operatsiooniriskide hindamise osana vastavalt EBA SREPi suuniste punkti 240 alapunktile j, et vältida tegevuse dubleerimist või mitmekordset arvestamist.

60. Eelkõige peaksid pädevad asutused hindama, kas krediidiasutusel või investeerimisühingul on kehtestatud tõhus raamistik IKTga seotud tegevuse edasiandmise riski tuvastamiseks, mõistmiseks ja mõõtmiseks ning kas on kehtestatud kontrollid ja kontrollikeskkond oluliste tellitud IKT-teenustega seotud riskide maandamiseks. See raamistik on krediidiasutuse või investeerimisühingu suurust, tegevust ja IKT-riskiprofiili arvestades proportsionaalne ning hõlmab järgmist:

a. IKTga seotud tegevuse edasiandmise riski mõju hindamine krediidiasutuse või investeerimisühingu riskijuhtimisele seoses teenusepakkujate (näiteks pilveteenuse pakkujate) ja nende teenustega hankemenetluse ajal, mis on dokumenteeritud ja mida kõrgem juhtkond või juhtorgan võtab teenuste tellimise üle otsustamisel arvesse. Krediidiasutus või investeerimisühing peaks vaatama läbi teenusepakkuja IKT-riski juhtimise põhimõtted ning IKT-kontrollimeetmed ja -kontrollikeskkonna veendumaks, et need vastavad tema riskijuhtimise sise-eesmärkidele ja riskivalmidusele. Seda läbivaatust tuleks lepingujärgse tegevuse edasiandmise perioodi vältel regulaarselt uuendada, võttes arvesse tellitavate teenuste omadusi;

b. tellitavate teenuste IKT-riskide jälgimine lepingujärgse tegevuse edasiandmise perioodi vältel krediidiasutuse või investeerimisühingu riskijuhtimise osana, mida kajastatakse krediidiasutuse või investeerimisühingu IKT-riski juhtimise aruandluses (näiteks talitluspidevuse või turvalisuse aruandlus);

c. saadud teenuse tasemete jälgimine ja võrdlus lepingus kokkulepitud tasemetega, mis peaks olema tegevuse edasiandmise lepingu või teenustaseme lepingu osa, ning

d. piisavalt töötajaid, ressursse ja pädevust tellitavate teenuste IKT-riskide järelevalveks ja haldamiseks.

3.4 Järelduste kokkuvõte ja punktiarvestus

61. Pärast eespool nimetatud hindamist peaks pädevatel asutustel kujunema arvamus krediidiasutuse või investeerimisühingu IKT-riski kohta. See arvamus peaks kajastuma järelduste kokkuvõttes, mida pädevad asutused peaksid arvestama EBA SREPi suuniste tabeli 6 operatsiooniriski punktisumma määramisel. Kujundades oma arusaamist olulistest IKT-riskidest, peaksid pädevad asutused võtma arvesse järgmisi operatsiooniriski hindamisel kasutatavaid kaalutlusi:

a. riskidega seotud kaalutlused

   i. krediidiasutuse või investeerimisühingu riskiprofiil ja riskide suurus;
   ii. tuvastatud olulised IKT-süsteemid ja teenused ning
   iii. oluliste IKT-süsteemidega seotud IKT-riski olulisus.

b. juhtimise ja kontrolliga seotud kaalutlused

   i. kas krediidiasutuse või investeerimisühingu IKT-riski juhtimise põhimõtted ja strateegia on kooskõlas tema üldstrateegia ja riskivalmidusega;
   ii. kas IKT-riski juhtimise raamistik on töökindel, selles on määratud selged vastutusvaldkonnad ning selgesti eraldatud riskide eest vastutajate ning juhtimis- ja kontrollifunktsiooni ülesanded;

iii. kas IKT-riski mõõtmise, järelevalve ja aruandluse süsteemid on asjakohased ning
iv. kas oluliste IKT-riskide kontrolliraamistikud on usaldusväärsed.

62. Kui pädevad asutused peavad IKT-riski oluliseks ning pädev asutus otsustab hinnata seda riski ja anda sellele punktid operatsiooniriski allkategooriana, siis on IKT-riski punktisumma kaalutlused esitatud allpool tabelis (tabel 1).

Tabel 1. IKT-riski punktisumma määramise järelevalvealased kaalutlused

Riski punktisumma	Järelevalveasutuse arvamus	Olemusliku riski kaalutlused	Nõuetekohase juhtimise ja kontrolli kaalutlused
1	Olemusliku riski ning juhtimise ja kontrolli taset arvestades krediidiasutuse või investeerimisühingu usaldatavusele avalduva olulise mõju märkimisväärne risk puudub.	• Punkti 37 kohaselt arvesse võetavad andmeallikad ei näidanud olulist avatust IKT-riskidele. • Krediidiasutuse või investeerimisühingu IKT-riskiprofiili olemus ja oluliste IKT-süsteemide ning IKT-süsteemidele ja -teenustele avalduvate oluliste IKT-riskide läbivaatamine ei toonud esile olulisi IKT-riske.	• Krediidiasutuse või investeerimisühingu IKT-riskide põhimõtted ja strateegia on tema üldstrateegiat ja riskivalmidust arvestades proportsionaalsed. • IKT-riski juhtimise raamistik on töökindel, selles on määratud selged vastutusvaldkonnad ja riskide eest vastutajate ning juhtimis- ja kontrollifunktsiooni ülesanded on selgesti eraldatud. • IKT-riski mõõtmise, järelevalve ja aruandluse
2	Olemusliku riski ning juhtimise ja kontrolli taset arvestades on krediidiasutuse või investeerimisühingu usaldatavusele olulise mõju avaldumise risk väike.	• Punkti 37 kohaselt arvesse võetavad andmeallikad ei näidanud olulist avatust IKT-riskidele. • Krediidiasutuse või investeerimisühingu IKT-riskiprofiili olemus ja oluliste IKT-süsteemide ning IKT-süsteemidele ja -teenustele avalduvate oluliste IKT-riskide läbivaatamine näitas piiratud IKT-riski (kuni 2 eelnevalt määratletud IKT-riski kategooriat 5st).	
3	Olemusliku riski ning juhtimise ja kontrolli taset arvestades on krediidiasutuse või investeerimisühingu usaldatavusele olulise mõju	• Punkti 37 kohaselt arvesse võetavad andmeallikad näitasid võimalikku olulist avatust IKT-riskidele. • Krediidiasutuse või investeerimisühingu IKT-riskiprofiili olemus ja oluliste	

	avaldumise risk keskmine.	IKT-süsteemide ning IKT-süsteemidele ja teenustele avalduvate oluliste IKT-riskide läbivaatamine näitas kõrgendatud IKT-riski (vähemalt 3 eelnevalt määratletud IKT-riski kategooriat 5st).	süsteemid on asjakohased. • IKT-riski kontrolliraamistik on usaldusväärne.
4	Olemusliku riski ning juhtimise ja kontrolli taset arvestades on krediidiasutuse või investeerimisühingu usaldatavusele olulise mõju avaldumise risk suur.	• Punkti 37 kohaselt arvesse võetavad andmeallikad näitasid mitmes punktis olulist avatust IKT-riskidele. • Krediidiasutuse või investeerimisühingu IKT-riskiprofiili olemus ja oluliste IKT-süsteemide ning IKT-süsteemidele ja -teenustele avalduvate oluliste IKT-riskide läbivaatamine näitas suurt IKT-riski (4 või 5 eelnevalt määratletud IKT-riski kategooriat 5st).	

Lisa. IKT-riskide klassifikatsioon

Viis IKT-riskide kategooriat koos mitteammendava loeteluga IKT-riskidest, mis võivad olla väga suured ja/või mõjutada toiminguid, mainet või millel on finantsmõju

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
IKT käideldavuse ja talitluspidevusega seotud riskid	Ebapiisav suutlikkuse haldus	Ressursside puudumine võib põhjustada võimetuse suurendada teenuse pakkumist tegevusvajaduste rahuldamiseks, süsteemi häireid, teenuse halvenemist ja/või vigu toimingutes.	• Võimsuse puudujääk võib mõjutada andmete edastuskiirust ja võrgu (interneti) kasutatavust teenuste, näiteks internetipanganduses. • (Enda või kolmanda isiku) töötajate puudus võib põhjustada süsteemi häireid ja/või vigu toimingutes.
	IKT-süsteemi tõrked	Käideldavuse vähenemine riistvara tõrgete tõttu.	• Salvestus- (kõvakettad), serveri- või muude IKT-seadmete tõrge/rike, mille põhjustab näiteks puudulik hooldus.
		Käideldavuse vähenemine tarkvara tõrgete või vigade tõttu.	• Lõpmatu silmus rakendustarkvaras ei võimalda tehingut teostada. • Kaasaegsetele käideldavuse ja vastupidavuse nõuetele enam mittevastavate ja/või pakkujapoolse toeta vananenud IKT-süsteemide ja -lahenduste jätkuvast kasutusest tulenevad katkestused.
	IKT talitluspidevuse ja avariitaaste ebapiisav kavandamine	IKT kavandatud käideldavuse ja/või talitluspidevuse lahenduste ja/või avariitaaste meetme (näiteks varuvariandi taastamise andmekeskuse) tõrge intsidentide korral aktiveerimisel.	• Seadistuse erinevused esmase ja teisese andmekeskuse vahel võivad põhjustada varu-andmekeskuse võimetuse tagada teenuse kavandatud talitluspidevus.
	Häirivad ja hävitavad küberründed	Mitmesugustel eesmärkidel (näiteks häkkimine või väljapressimine) tehtavad ründed, mis võivad põhjustada süsteemide ja võrgu ülekoormuse ning	• Hajusaid teenusetõkestusründe ihakse suure hulga häkkeri kontrollitavate arvutisüsteemide abil

[10] IKT-riskid on loetletud kõige rohkem mõjutatud riskikategooria all, kuid need võivad mõjutada ka teisi kategooriaid

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
		muuta arvutiteenustele juurdepääsu seaduslike kasutajate jaoks võimatuks.	internetis, saates internetiteenustele (näiteks elektroonilistele pangateenustele) suurel arvul näiliselt õiguspäraseid teenusetaotluseid.
IKT-turvariskid	Küberründed ja teised organisatsioonivälised IKT-põhised ründed	Internetist või välisvõrkudest eri eesmärkidel (näiteks pettus, spionaaž, häkkerlus/sabotaaž, küberterrorism) ning mitmesuguste meetoditega (näiteks sotsiaalne manipulatsioon, sissetungikatsed haavatavuste ärakasutamise teel, pahavara kasutamine) tehtavad rünnakud, mille tagajärjel saadakse kontroll IKT-sisesüsteemide üle.	Erinevad ründe liigid: • kinnisründeoht – sisesüsteemide üle kontrolli saamiseks ja teabe varastamiseks (näiteks identiteedi-, krediitkaarditeabe varastamiseks); • pahavara (näiteks lunaraha nõudev tarkvara), mis krüpteerib andmeid väljapressimise eesmärgil; • organisatsioonisiseste IKT-süsteemide nakatamine Trooja hobustega, et teha varjatult pahatahtlikke süsteemitoiminguid; • IKT-süsteemide ja/või (veebi)rakenduste haavatavuse ärakasutamine (näiteks SQL-süst), et saada juurdepääs organisatsioonisisesele IKT-süsteemile.
		Ebaseaduslike maksetehingute tegemine häkkerite poolt, murdes läbi või hiilides mööda elektrooniliste panga- ja makseteenuste turvameetmetest ja/või rünnates ja kasutades ära krediidiasutuse või investeerimisühingu sisese maksesüsteemi turvalünki.	• Ründed elektrooniliste panga- ja makseteenuste vastu, et teha volitamata tehinguid. • Petturlike maksetehingute loomine ja väljasaatmine krediidiasutuse või investeerimisühingu sisemaksesüsteemides (näiteks petturlikud SWIFT-sõnumid).
		Petturlike väärtpaberitehingute tegemine häkkerite poolt, murdes läbi või hiilides mööda elektrooniliste pangateenuste turvameetmetest, mis võimaldavad juurdepääsu ka klientide väärtpaberikontodele.	• „Pump and dump“ ründed, millega häkkerid saavad juurdepääsu klientide elektroonilistele väärtpaberikontodele ja esitavad petturlikke ostu- või müügitellimusi, et mõjutada turuhinda ja/või teenida kasumit varem võetud väärtpaberipositsioonidelt.
		Kõikvõimalike IKT-süsteemide sideühenduste ja suhtluse ründamine, et koguda teavet ja/või sooritada pettust.	• Kaitsmata lihtteksti kujul autentimisandmete edastuse pealtkuulamine/kinnipüüdmine.

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
	Ebapiisav organisatsioonisisene IKT turvalisus	Krediidiasutuselt või investeerimisühingult volitamata juurdepääsu saamine olulistele IKT-süsteemidele mitmesugustel eesmärkidel (näiteks pettus, petturlike kauplemistehingute teostamine ja varjamine, andmevargus, aktivism/sabotaaž) ja eri meetoditega (näiteks privileegide kuritarvitamine ja/või eskaleerumine, identiteedivargus, sotsiaalne manipulatsioon, IKT-süsteemide haavatavuste ärakasutamine, pahavara kasutamine).	• Klahvilogerite paigaldamine eesmärgiga varastada kasutajate kasutajatunnuseid ja salasõnu, et saada volitamata juurdepääsu konfidentsiaalsetele andmetele ja/või sooritada pettust. • Nõrkade salasõnade murdmine/äraarvamine, et saada ebaseaduslikke või kõrgemaid juurdepääsuõiguseid. • Süsteemihaldur kasutab operatsioonisüsteeme või (andmebaasi vahetuks muutmiseks ettenähtud) andmebaasivahendeid pettuse sooritamiseks.
		Volitamata IKT manipulatsioonid, mis tulenevad ebasobivatest IKT juurdepääsu halduse menetlustest ja tavadest.	• Võimetus blokeerida või kustutada mittevajalikke kontosid, näiteks kui töötaja funktsioon on muutunud ja/või ta on krediidiasutusest või investeerimisühingust lahkunud, sh külalised või tarnijad, kes enam juurdepääsu ei vaja, mistõttu saadakse volitamata juurdepääs IKT-süsteemidele. • Ülemääraste juurdepääsuõiguste ja -privileegide andmine, mis võimaldab volitamata juurdepääsu ja/või petturlike tegevuste varjamist.
		Turvariskid, mis tulenevad turbeteadlikkuse vähesusest, kui töötajad ei saa IKT turvapõhimõtetest ja -menetlustest aru, ei arvesta või ei järgi neid.	• Töötajad, kes meelitatakse rünnet abistama (näiteks sotsiaalse manipulatsiooniga). • Pääsumandaatidega seotud tavade nõrkus: salasõnade jagamine, kergesti äraarvatavate salasõnade kasutamine, sama salasõna kasutamine eri otstarvetel jne. • Krüpteerimata konfidentsiaalsete andmete hoidmine sülearvutites või kaasaskantavatel andmekandjatel (näiteks USB-võtmetel), mis võivad kaduma minna või mida võidakse varastada.
		Konfidentsiaalse teabe volitamata talletamine või edastamine väljaspool krediidiasutust või	• Isikud varastavad või lekitavad või viivad konfidentsiaalset teavet tahtlikult välja volitamata

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
		investeerimisühingut.	isikutele või avalikkusele.
	Ebapiisav füüsiline IKT turvalisus	IKT-varade väärkasutus või vargus füüsilise juurdepääsu teel, põhjustades kahju, varade või andmete kaotust või muutes võimalikuks muud ohud.	• Füüsiline sissetung büroohoonetesse ja/või andmekeskustesse eesmärgiga varastada IKT-seadmeid (näiteks laua- või sülearvuteid või salvestusseadmeid) ja/või kopeerida andmeid IKT-süsteemidele füüsiliselt ligi pääsedes.
		IKT-varadele tahtlik või tahtmatu kahju tekitamine, mida põhjustavad terrorism, õnnetused või krediidiasutuse või investeerimisühingu töötajate ja/või kolmandate isikute (tarnijate, parandajate) soovimatud või ekslikud manipulatsioonid.	• Füüsiline terrorism (näiteks terroristide pommid) või IKT-varade saboteerimine. • Tulekahjust, veelekkest või muudest teguritest põhjustatud andmekeskuse hävimine.
		Ebapiisav füüsiline kaitse loodusõnnetuste vastu, mis põhjustab IKT-süsteemide / -andmekeskuste osalise või täieliku hävimise loodusõnnetuse korral.	• Maavärinad, äärmuslik kuumus, tuuletormid, tugevad lumetormid, üleujutused, tulekahjud, äike.
IKT-muutustega seotud riskid	Ebapiisav kontroll IKT-süsteemi muutuste ja IKT-arenduse üle	Avastamata vigadest või haavatavustest põhjustatud intsidendid (näiteks muutuse ettenägematu mõju või muutuse puudulik haldamine testide puudumise tõttu või ebaõiged muutuste haldamise tavad) tarkvaras, IKT-süsteemides ja andmetes.	• Ebapiisavalt testitud tarkvara või seadistuse muutuste kasutuselevõtt, mis avaldab ettenägematut kahjulikku mõju andmetele (näiteks rikkumine, kustutamine) ja/või IKT-süsteemi toimivusele (näiteks süsteemi kokkukukkumine või toimivuse halvenemine). • IKT-süsteemide või andmete kontrollimatud muutused tootmiskeskkonnas. • Halvasti turvatud IKT-süsteemide ja internetirakenduste kasutuselevõtt, luues häkkeritele võimalusi rünnata pakutavaid internetiteenuseid ja/või murda sisse organisatsioonisisestesse IKT-süsteemidesse. • Organisatsioonisiseselt arendatava tarkvara lähtekoodi kontrollimatu muutmine. • Ebapiisav testimine, mis tuleneb piisava testimiskeskkonna puudumisest.

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
	Ebapiisav IKT-arhitektuur	IKT-arhitektuuri puudulik haldus IKT-süsteemide (näiteks tarkvara, riistvara, andmete) projekteerimisel, loomisel ja haldamisel võib anda aja jooksul komplekssed, keerulised, suurte halduskuludega ja jäigad IKT-süsteemid, mis ei ole enam ärivajadustega piisavalt kooskõlas ja ei täida tegelikke riskijuhtimise vajadusi.	• Aja jooksul halvasti juhitud muudatused IKT-süsteemides, tarkvaras ja/või andmetes, mille tulemuseks on komplekssed, heterogeensed ja raskesti hallatavad IKT-süsteemid ja -arhitektuurid, mis avaldab mitmesugust kahjulikku mõju äritegevusele ja riskijuhtimisele (näiteks paindlikkuse ja reageerimisvõime puudumine, IKT-intsidendid ja -tõrked, suured käitamiskulud, nõrgenenud IKT turvalisus ja vastupidavus, vähenenud andmete kvaliteet ja aruandlusvõimekus). • Kommertstarkvarapakettide ülemäärane kohandamine ja laiendamine organisatsioonisiseselt arendatava tarkvaraga, mis põhjustab võimetuse juurutada kommertstarkvara tulevasi väljalaskeid ja täiustusi ning riski jääda tootja toeta.
	Ebasobiv elutsükli ja paikade haldus	Võimetus hallata kõigi IKT-varade ülevaadet, mis toetaks usaldusväärseid elutsükli ja paikade haldustavasid ja oleks nendega ühendatud. Selle tulemuseks on ebapiisavalt paigatud (ja seetõttu haavatavamad) ning vananenud IKT-süsteemid, mis ei pruugi toetada äritegevus- ja riskijuhtimisvajadusi.	• Paikamata ja vananenud IKT-süsteemid võivad avaldada negatiivset mõju äritegevusele ja riskijuhtimisele (näiteks paindlikkuse ja reageerimisvõime puudumine, IKT katkestused, nõrgenenud IKT turvalisus ja vastupidavus).
IKT andmeterviklus e riskid	Vigane IKT-andmete töötlus või käitlus	Süsteemi, side ja/või rakenduse vigade või tõrgete või valesti teostatud andmete väljavõtte, edastamise või laadimise protsessi tõttu võivad andmed saada rikutud või minna kaduma.	• IT-süsteemi viga pakktöötlusel, mis põhjustab kliendi pangakontol ebaõigeid seise. • Valesti teostatud päringud. • Andmete dubleerimise (varundamise) veast tulenev andmekadu.
	Valesti projekteeritud andmete valideerimiskontr	Vead, mis tulenevad puuduvatest või ebatõhusatest andmesisestuse ja vastuvõtu automaatkontrollidest (näiteks kasutatud kolmandate isikute andmete korral) või andmete edastuse, töötluse või väljastamise	• Sisendandmete ebapiisav või mittekehtiv vormindamine/valideerimine rakendustes ja/või kasutajaliidestes. • Andmete kooskõlastuse kontrollide või nende

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
	oll IKT-süsteemides.	kontrollidest IKT-süsteemides (näiteks sisendandmete valideerimiskontrollid ja andmete kooskõlastamine).	väljundite puudumine. • Andmete väljavõtuprotsesside (näiteks andmebaasipäringute) kontrollide puudumine, mis põhjustab vigaseid andmeid. • Vigaste välisandmete kasutamine.
	Valesti kontrollitud andmete muutused IKT-tootmissüsteemides	Andmevead, mis tulenevad IKT-süsteemide kasutamisel tehtud andmemanipulatsioonide nõuetekohasuse ja põhjendatuse kontrollide puudumisest.	• Arendajad või andmebaasihaldurid hindavad ja muudavad IKT-tootmissüsteemides andmeid vahetult ja mittekontrollitavalt, näiteks IKT-intsidendi korral.
	Valesti projekteeritud ja/või hallatud andmearhitektuur, andmevood, andmemudelid või andmesõnastikud	Valesti hallatud andmearhitektuurid, andmemudelid, andmevood või andmesõnastikud võivad põhjustada samade andmete erinevaid versioone IKT-süsteemides, mis ei ole erinevalt rakendatavate andmemudelite või andmemääratluste ja/või andmete loomise ja muutmise alusprotsesside erinevuste tõttu enam omavahel sidusad.	• Toote- või kliendiüksuste erinevad kliendiandmebaasid, kus on erinevad andmemääratlused ja -väljad ja millest tulenevad kooskõlastamatud ning krediidiasutuse või investeerimisühingu tasandil raskesti võrreldavad ja integreeritavad kliendiandmed.
IKTga seotud tegevuse edasiandmise riskid	Kolmanda isiku või kontserni teise üksuse teenuste ebapiisav vastupidavus	Oluliste IKT-teenuste, telekommunikatsiooniteenuste ja kommunaalteenuste kättesaamatus. Teenusepakkujale usaldatud oluliste/tundlike andmete kadumine või rikkumine.	• Põhiteenuste kättesaamatus tulenevalt tarnijate (edasiantud) IKT-süsteemide või -rakenduste riketest. • Telekommunikatsiooniühenduste häired. • Elektritoite puudus.
	Tegevuse edasiandmise halduse ebapiisavus	Teenuse oluline halvenemine või häiritus tulenevalt tellitud teenuse pakkuja ebapiisavast valmisolekust või kontrolliprotsessist. Tegevuse edasiandmise ebapiisav haldus võib põhjustada puudujääke oskustes ja võimekuses tuvastada, hinnata, maandada ja jälgida täielikult IKT-riske ning piirata krediidiasutuse või investeerimisühingu tegevussuutlikkust.	• Teenusepakkumise lepingus hõlmatud intsidentide menetlemise korra, lepinguliste kontrollimehhanismide ning tagatiste puudulikkus, mis suurendab võtmeisikute sõltuvust kolmandatest isikutest ja teenusepakkujatest. • Ebasobivad muutuste haldamise kontrollid teenusepakkuja IKT-keskkonnas võivad põhjustada teenuse olulise halvenemise või tõrke.

IKT-riskide kategooriad	IKT-riskid (mitteammendav loetelu)[10]	Riski kirjeldus	Näited
	Kolmanda isiku või kontserni teise üksuse ebapiisav turvalisus	Kolmandast isikust teenusepakkujate IKT-süsteemide häkkimine, mis mõjutab otseselt tellitud teenuseid või teenusepakkuja juures hoitavaid olulisi ja tundlikke andmeid. Teenusepakkuja töötajad saavad volitamata juurdepääsu teenusepakkuja juures hoitavatele olulistele ja tundlikele andmetele.	• Teenusepakkujate häkkimine kurjategijate või terroristide sisenemispunktina krediidiasutuse või investeerimisühingu IKT-süsteemidesse või selleks, et pääseda ligi teenusepakkuja juures hoitavatele olulistele ja tundlikele andmetele või neid hävitada. • Teenusepakkuja siseringi pahatahtlikud liikmed püüavad varastada ja müüa tundlikke andmeid.