Suunised

EBA/GL/2019/04

28. november 2019

EBA suunised IKT- ja turvariskide juhtimiseks

Vastavus- ja aruandluskohustused

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

Teatamisnõuded

3. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama hiljemalt ([pp.kk.aaaa]) EBA-le, kas nad järgivad või kavatsevad järgida kõnealuseid suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei laeku, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleks saata EBA veebilehel avaldatud ankeediga aadressil compliance@eba.europa.eu, märkides viiteks „EBA/GL/2019/04“. 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 nr 1093/2010 artikli 16 lõikega 3 avaldatakse teated Euroopa Pangandusjärelevalve veebilehel.

[1] Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, 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).

Sisu, kohaldamisala ja mõisted

Sisu

5. Suunised põhinevad direktiivi 2013/36/EL (kapitalinõuete direktiiv) artikli 74 sätetel seoses sisemise juhtimissüsteemiga ja tulenevad direktiivi 2015/2366/EL (teine makseteenuste direktiiv) artikli 95 lõikes 3 sätestatud volitusest suuniseid väljastada.

6. Nendes suunistes sätestatakse riskide juhtimise meetmed, mida finantseerimisasutused (määratletud allpool lõikes 9) peavad võtma kapitalinõuete direktiivi artikli 74 kohaselt, et juhtida oma IKT- ja turvariske kõigi tegevuste puhul ja mida makseteenuse pakkujad (määratletud allpool lõikes 9) peavad võtma teise makseteenuste direktiivi artikli 95 lõike 1 kohaselt, et juhtida nende osutatavate makseteenustega seotud operatsiooni- või turvariske (mida käsitletakse „IKT- ja turvariskidena“). Need suunised sisaldavad infoturbe, sh küberturbe nõudeid teabele, mida hoiustatakse IKT-süsteemides.

Kohaldamisala

7. Suuniseid kohaldatakse finantseerimisasutustes (määratletud lõikes 9) IKT- ja turvariskide juhtimisele. Käesolevates suunistes tähendab mõiste „IKT- ja turvariskid“ teise makseteenuste direktiivi artikli 95 operatsiooni- ja turvariske makseteenuste osutamisel.

8. Makseteenuse pakkujatele (määratletud lõikes 9) kohaldatakse neid suuniseid makseteenuste osutamisel kooskõlas teise makseteenuste direktiivi artikli 95 rakendusala ja volitusega. Asutuste (määratletud lõikes 9) puhul kohaldatakse neid suuniseid kõigile nende pakutavatele tegevustele.

Adressaadid

9. Suunised on adresseeritud finantseerimisasutustele, mis tähendab suunistes (1) teise makseteenuste direktiivi artikli 4 lõikes 11 määratletud makseteenuse pakkujaid ja (2) määruse (EL) nr 575/2013 artikli 4 lõike 1 punktis 3 määratletud asutusi, st krediidiasutusi ja investeerimisühinguid. Käesolevaid suuniseid kohaldatakse ka määruse (EL) nr 575/2013 artikli 4 lõike 1 punktis 40 määratletud pädevatele asutustele, sealhulgas Euroopa Keskpangale seoses ülesannetega, mis on talle antud määrusega (EL) nr 1024/2013, ning pädevatele asutustele teise makseteenuste direktiivi kohaselt, millele on osutatud määruse (EL) nr 1093/2010 artikli 4 lõike 2 alapunktis i.

Mõisted

10. Kui ei ole sätestatud teisiti, on kapitalinõuete direktiivis 2013/36/EL, määruses (EL) nr 575/2013 ja direktiivis 2015/2366/EL (teine makseteenuste direktiiv) kasutatud ja määratletud mõistetel sama tähendus ka käesolevates suunistes. Lisaks kasutatakse suunistes järgnevaid mõisteid.

IKT- ja turvarisk	Konfidentsiaalsuse rikkumisest, süsteemide ja andmete usaldusväärsusega seotud tõrgetest, süsteemide ja andmete sobimatusest või mittekättesaadavusest või võimetusest muuta infotehnoloogiat (IT) mõistliku aja jooksul ja kuludega, kui keskkond või äritegevuse nõuded muutuvad (st võimekus), tekkiva kahju risk [2]. See hõlmab turvariske, mis tulenevad ebapiisavatest või nurjunud ettevõttesisestest protsessidest või välistest sündmustest, sh küberrünnakutest või ebapiisavast füüsilisest turvalisusest.
Juhtorgan	(a) Krediidiasutuste ja investeerimisühingute jaoks on selle termini tähendus sama kui direktiivi 2013/36/EL artikli 3 lõike 1 punkti 7 määratluses. (b) Makseasutuste või e-raha asutuste jaoks tähendab see termin juhtkonda või teisi makseasutuse või e-raha asutuse juhtimise eest vastutavaid isikuid ja (kui asjakohane) isikuid, kes vastutavad makseasutuste või e-raha asutuste juures makseteenustega seotud tegevuste eest. (c) Direktiivi (EL) 2015/2366 artikli 1 lõike 1 punktides c, e ja f nimetatud makseteenuse pakkujate jaoks on sellel terminil tähendus, mis omistatakse sellele kohalduva Euroopa Liidu või liikmesriigi õigusega.
Operatsiooniriski- või turvaintsident	Sündmus või mitu seotud sündmust, mida finantseerimisasutus ei ole kavandanud, mis kahjustavad või tõenäoliselt kahjustavad teenuste terviklikkust, käideldavust, konfidentsiaalsust ja/või autentsust.
Kõrgem juhtkond	(a) Krediidiasutuste ja investeerimisühingute jaoks on selle termini tähendus sama kui direktiivi 2013/36/EL artikli 3 lõike 1 punkti 9 määratluses. (b) Makseasutuste ja e-raha asutuste jaoks tähendab see termin füüsilisi isikuid, kes täidavad asutuses juhtimiskohustusi ning kes vastutavad ja on aruandekohustuslikud juhtorgani ees asutuse igapäevase juhtimise eest. (c) Direktiivi (EL) 2015/2366 artikli 1 lõike 1 punktides c, e ja f nimetatud makseteenuse pakkujate jaoks on sellel terminil tähendus, mis omistatakse sellele kohalduva Euroopa Liidu või liikmesriigi õigusega.
Riskiisu	Nende riskide agregeeritud tase ja tüüp, mida makseteenuse pakkujad ja asutused on kooskõlas oma ärimudeliga valmis riskitaluvusvõime piires strateegiliste eesmärkide saavutamiseks võtma.

[2] EBA 19. detsembri 2014 suunistest pärit järelevalvealase läbivaatamise ja hindamise protsessi ühiste menetluste ja metoodikate määratlus (EBA/GL/2014/13), muudetud dokumendiga EBA/GL/2018/03.

Auditi funktsioon	(a) Krediidiasutuse ja investeerimisühingute puhul on auditi funktsioon sama nagu see, millele viidatakse EBA sisemise juhtimissüsteemi suuniste jaos 22 (EBA/GL/2017/11). (b) Muudel makseteenuse pakkujatel peale krediidiasutuste peab auditi funktsioon olema makseteenuse pakkuja siseselt või pakkujast sõltumatu ning võib olla kas sisene ja/või väline auditi funktsioon.
IKT-projektid	Kõik projektid või nende osad, milles IKT-süsteeme ja teenuseid muudetakse, asendatakse, kõrvaldatakse või rakendatakse. IKT-projektid võivad olla osa laiemast IKT või äri ümberkujundamisprotsessist.
Kolmas isik	Organisatsioon, mis on sõlminud üksusega ärisuhte või lepingu toote või teenuse pakkumiseks[3].
Infovara	Kaitsmist vääriva ainelise või mitteainelise teabe kogum.
IKT-vara	Ärikeskkonnas leiduv tark- või riistvara.
IKT-süsteemid[4]	IKT-kogum kui osa mehhanismist või omavahel ühendatud võrgustikust, mis toetab finantseerimisasutuse tegevusi.
IKT-teenused[5]	IKT-süsteemide osutatavad teenused ühele või enamale sisesele või välisele kasutajale. Näideteks on andmesisestus, andmesalvestus, andmetöötluse ja aruandluse teenused, aga ka seire ning äri ja otsuste tegemise tugiteenused.

Rakendamine

Kohaldamise alguskuupäev

11. Käesolevaid suuniseid kohaldatakse alates 30. juunist 2020.

Kehtetuks tunnistamine

12. Nende suunistega tunnistatakse kuupäeval, mil suuniseid kohaldama hakatakse, kehtetuks 2017. aastal väljastatud operatsiooni- ja turvariskide turvameetmete suunised (EBA/GL/2017/17).

[3] Määratlus G7 kolmandate isikute küberriski juhtimise põhielementidest finantssektoris.
[4] Määratlus suunistest info- ja kommunikatsioonitehnoloogia riskide hindamise kohta järelevalvealase läbivaatamise ja hindamise protsessi raames (SREP) (EBA/GL/ 2017/05).
[5] *ibid*.

IKT- ja turvariskide juhtimise suunised

1.1. Proportsionaalsus

1. Kõik finantseerimisasutused peaksid pidama kinni käesolevate suuniste sätetest viisil, mis on proportsionaalne ja arvestab finantseerimisasutuse suuruse, ettevõttesisese korralduse ning nende finantseerimisasutuste teenuste ja toodete olemuse, rakendusala, keerukuse ja riskitasemega, mida asutus pakub või kavatseb pakkuda.

1.2. Juhtimiskord ja strateegia

1.2.1. Juhtimiskord

2. Juhtorgan peaks tagama, et finantseerimisasutustel on IKT- ja turvariskide jaoks kehtestatud piisav sisemine juhtimissüsteem ja sisekontrolliraamistik. Juhtorgan peaks sätestama IKT-funktsioonide, infoturbe riskijuhtimise ja talitluspidevuse, sh juhtorgani ja selle komiteede jaoks selged rollid ja kohustused.
3. Juhtorgan peab tagama, et finantseerimisasutuste töötajate arv ja oskused on piisavad nende IKT-alaste toimingute ning IKT- ja turvariski juhtimise protsesside järjepidevaks toetamiseks ning IKT-strateegia rakendamise tagamiseks. Juhtorgan peaks tagama, et eraldatud eelarve on eelmainitu täitmiseks piisav. Finantseerimisasutused peaks lisaks tagama, et kõik töötajad, sh võtmeisikud saavad igal aastal või vajadusel sagedamini IKT ja turvariskide, sh infoturbe alal nõuetekohast väljaõpet (vt ka jagu 1.4.7).
4. Juhtorganil on üldine vastutus finantseerimisasutuste IKT-strateegia kehtestamise, kinnitamise ja rakendamise üle osana nende üldisest äristrateegiast ning tõhusa IKT- ja turvariskide riskijuhtimise raamistiku kehtestamise eest.

1.2.2. Strateegia

5. IKT-strateegia peaks olema vastavuses finantseerimisasutuse üldise äristrateegiaga ning selles peaks olema määratletud järgnev:
    a) kuidas finantseerimisasutuse IKT peaks arenema, et äristrateegiat tõhusalt toetada ja selles osaleda, sh organisatsioonilise struktuuri areng, IKT-süsteemide muudatused ja peamised sõltuvused kolmandatest isikutest;
    b) IKT-arhitektuuri kavandatud strateegia ja areng, sh sõltuvus kolmandatest isikutest;
    c) selged infoturbe eesmärgid, mis keskenduvad IKT-süsteemidele, IKT-teenustele, töötajatele ja protsessidele.
6. Finantseerimisasutused peaksid kehtestama tegevuskavad, mis sisaldavad IKT-strateegia eesmärgi täitmiseks võetavaid meetmeid. Need tuleb edastada kõigile seotud töötajatele (sh kohaldatavatel ja asjakohastel juhtudel töövõtjatele ja kolmandast isikust teenuseosutajatele). Tegevuskavasid tuleb regulaarselt üle vaadata, veendumaks, et need on asjakohased ja

nõuetekohased. Finantseerimisasutused peaksid kehtestama protsessid oma IKT-strateegia rakendamise tõhususe jälgimiseks ja mõõtmiseks.

1.2.3. Kolmandast isikust teenuseosutajate kasutamine

7. Piiramata EBA suuniseid tegevuse edasiandmise kokkulepete alal (EBA/GL/2019/02) ja teise makseteenuste direktiivi artiklit 19, peavad finantseerimisasutused tagama riski juhtimise raamistikus määratletud riski juhtimise meetmete, sh käesolevates suunistes sätestatud meetmete tõhususe, kui makseteenuste operatiivseid funktsioone ja/või IKT-teenuseid ning mis tahes tegevuse IKT-süsteeme ostetakse sisse, sh kontserni ettevõtetele, või kui kasutatakse kolmandaid isikuid.
8. IKT-teenuste ja IKT-süsteemide talitluspidevuse tagamiseks peaksid finantseerimisasutused lisama teenuseosutajatega (sisseostetava teenuse pakkujad, kontserni ettevõtted või kolmandast isikust teenuseosutajad) sõlmitavatesse lepingutesse ja teenustaseme lepingutesse (nii tavatingimustel kui teenuse katkemise korral – vt ka jagu 3.7.2) järgmise:
    a) nõuetekohased ja proportsionaalsed infoturbega seotud eesmärgid ja meetmed, sh sellised nõuded nagu küberturvalisuse miinimumnõuded; finantseerimisasutuse andmete elutsükli kirjeldus; mis tahes nõuded seoses andmete krüpteerimise, võrguturvalisuse ja turvalisuse seireprotsessidega ning andmekeskuste asukoht;
    b) operatsiooni- ja turvariskide juhtimise protseduurid, sh eskaleerimine ja aruandlus.
9. Finantseerimisasutused peaksid jälgima ja kindlaks tegema, kuidas ja mis tasemel järgivad sellised teenusepakkujad finantseerimisasutuse turvaeesmärke, -meetmeid ja -toimimiseesmärke.

1.3. IKT- ja turvariskide juhtimisraamistik

1.3.1. Korraldus ja eesmärgid

10. Finantseerimisasutused peaksid tuvastama ja haldama oma IKT- ja turvariske. IKT-süsteemide, -protsesside ja -turvategevuste eest vastutavatel IKT-funktsioonidel peavad olema kehtestatud asjakohased protsessid ja kontrollid tagamaks, et kõiki riske tuvastatakse, analüüsitakse, mõõdetakse, jälgitakse ja juhitakse, neist teavitatakse ning need jäävad finantseerimisasutuse riskiisu piiresse, nende tarnitavad projektid ja süsteemid ning tehtavad toimingud vastavad välistele ja sisestele nõuetele.
11. Finantseerimisasutused peaksid määrama vastutuse IKT- ja turvariskide juhtimise ning järelevalve eest kontrollifunktsioonile, järgides EBA sisemise juhtimissüsteemi (EBA/GL/2017/11) suuniste jao 19 nõudeid. Finantseerimisasutused peavad tagama selle kontrollfunktsiooni sõltumatuse ja erapooletuse, eraldades selle asjakohaselt IKT tööprotsessidest. Kontrollfunktsioonil peaks olema otsene aruandekohuslus juhtorgani ees ning see peaks vastutama IKT- ja turvariskide juhtimise raamistiku järgimise jälgimise ja kontrollimise eest. See peaks tagama, et IKT- ja turvariske tuvastatakse, mõõdetakse, hinnatakse, juhitakse ja jälgitakse ning neist teavitatakse. Finantseerimisasutused peaksid tagama, et see kontrollfunktsioon ei vastuta mis tahes siseauditi eest.

Riskipõhise lähenemise kohaselt peaks siseauditi suutma iseseisvalt läbi vaadata ja anda objektiivse kinnituse, et kõik IKT- ja turvalisusega seotud toimingud ning finantseerimisasutuse üksused peavad kinni finantseerimisasutuse poliitikatest ja protseduuridest ning välistest nõuetest EBA sisemise juhtimissüsteemi suuniste (EBA/GL/2017/11) jao 22 nõuete kohaselt.

12. Finantseerimisasutused peaksid piiritlema ja määrama peamised rollid ning vastutused ja asjakohased aruandlusahelad, et IKT- ja turvariski juhtimise raamistik oleks tõhus. See raamistik peaks olema täielikult integreeritud ja vastavusse viidud finantseerimisasutuse üldise riskijuhtimisprotsessiga.

13. IKT- ja turvariskide juhtimise raamistikus peaksid olema kehtestatud protsessid:

    a) IKT- ja turvariskide riskiisu kindlaks määramiseks vastavuses finantseerimisasutuse riskiisuga;
    b) nende IKT- ja turvariskide tuvastamiseks ja hindamiseks, millega finantseerimisasutus kokku puutub;
    c) leevendusmeetmete, sh kontrollide määratlemiseks, et IKT- ja turvariske leevendada;
    d) nende meetmete tõhususe ja teavitatud intsidentide, sh makseteenuse pakkujate puhul intsidentide, millest on teavitatud kooskõlas teise makseteenuste direktiiv artikliga 96 ja mis mõjutavad IKT-ga seotud toiminguid, jälgimiseks ning vajadusel meetmete parandamiseks;
    e) juhtorgani teavitamiseks IKT- ja turvariskide ja meetmete osas;
    f) tuvastamiseks ja hindamiseks, kas IKT-süsteemis või IKT-teenustes, -protsessides või -protseduurides toimunud suure muudatusega kaasneb IKT- ja turvariske ja/või muid märkimisväärseid operatsiooni- ja turvaintsidente.

14. Finantseerimisasutused peaksid tagama, et IKT- ja turvariskide juhtimise raamistik on dokumenteeritud ning seda täiustatakse pidevalt raamistiku rakendamisel ja seirel saadud kogemuste põhjal. Juhtorgan peaks IKT- ja turvariskide juhtimise raamistiku vähemalt korra aastas heaks kiitma ja üle vaatama.

1.3.2. Toimingute, protsesside ja varade tuvastamine

15. Finantseerimisasutused peaksid tuvastama, kehtestama ja säilitama oma ärifunktsioonide, rollide ja tugiprotsesside ajakohase kaardistuse, et selgitada välja neist igaühe olulisuse ja nende omavahelised seosed IKT- ja turvariskide osas.

16. Lisaks peaksid finantseerimisasutused tuvastama, looma ja säilitama nende ärifunktsioone toetavate infovarade ja tugiprotsesside, näiteks IKT-süsteemide, töötajate, töövõtjate, kolmandate isikute ning teistest sisestest ja välistest protsessidest sõltuvuse ajakohast kaardistust, et nad suudaksid vähemalthallata nende kriitilisi ärifunktsioone ja protsesse toetavaid infovarasid

1.3.3. Liigitamine ja riski hindamine

17. Finantseerimisasutused peaksid liigitama jagudes 15 ja 16 viidatud tuvastatud ärifunktsioone, tugiprotsesse ja infovarasid nende kriitilisuse alusel.

18. Tuvastatud ärifunktsioonide, tugiprotsesside ja infovarade kriitilisuse määratlemiseks peaksid finantseerimisasutused arvestama vähemalt konfidentsiaalsuse, andmetervikluse ja käideldavuse nõuetega. Infovaradele tuleks selgelt määrata aruandekohuslus ja vastutus.
19. Finantseerimisasutused peaksid riski hindamisel vaatama üle infovarade ja asjakohaste dokumentide liigitamise piisavuse.
20. Finantseerimisasutused peaksid kriitilisuse alusel tuvastama need IKT- ja turvariskid, mis mõjutavad tuvastatud ja liigitatud ärifunktsioone, tugiprotsesse ning infovarasid. Riskihindamist tuleb teha ja dokumenteerida igal aastal või vajadusel tihedamini. Riskihindamist tuleks lisaks teha taristus toimuvate või ärifunktsioone, tugiprotsesse või infovarasid mõjutavate protsesside või protseduuride suurte muudatuste puhul ning pärast seda finantseerimisasutuse olemasolevat riskihinnangut ajakohastada.
21. 21. Finantsasutused peaksid tagama, et nad jälgivad pidevalt oma äriprotsesside, tugifunktsioonide ja infovaradega seotud ohte ja haavatavusi, ning peaksid regulaarselt üle vaatama neid mõjutavaid riskistsenaariume.

1.3.4. Riski maandamine

22. Finantseerimisasutused peaksid riskihindamiste põhjal määrama kindlaks tuvastatud IKT- ja turvariskide vastuvõetavale tasemele maandamiseks vajalikud meetmed ja selle, kas olemasolevates äriprotsessides, kontrollimeetmetes, IKT-süsteemides ja IKT-teenustes on vaja teha muudatusi. Finantseerimisasutus peaks arvestama nende muudatuste rakendamiseks vajaliku aja ning ajutiste maandamismeetmete võtmiseks vajaliku ajaga, et minimeerida IKT- ja turvariske ning jääda finantseerimisasutuse IKT- ja turvariskiisu piiresse.
23. Finantseerimisasutused peaksid määrama kindlaks ja rakendama meetmeid tuvastatud IKT- ja turvariskide maandamiseks ning infovarade kaitsmiseks kooskõlas nende liigitusega.

1.3.5. Aruandlus

24. Finantseerimisasutused peaksid esitama juhtorganile riskihindamise tulemuste kohta selgeid ja ajakohaseid aruandeid. Need aruanded ei piira makseteenuste osutajate kohustust esitada pädevatele asutustele ajakohastatud ja põhjalik riskihinnang direktiivi (EL) 2015/2366 artikli 95 lõike 2 alusel.

1.3.6. Audit

25. Piisavate IKT- ja turvariskide ning maksete (makseteenuste osutajate puhul) alaste teadmiste, oskuste ja kogemustega audiitorid peavad regulaarselt viima läbi finantseerimisasutuste IKT- ja turvariskide juhtimise, süsteemide ja protsesside auditeid, et esitada juhtorganile sõltumatut kinnitust nende tõhususe kohta. Audiitorid peaksid olema finantseerimisasutusest või selle siseselt sõltumatud. Nende auditite sagedus ja fookus peaksid olema proportsionaalsed asjakohaste IKT- ja turvariskidega.
26. Finantseerimisasutuse juhtorgan peaks auditi plaani, sh IKT-auditid ning nende olulised muudatused heaks kiitma. Auditi plaan ja selle elluviimine, sh auditi sagedus peaksid kajastama

finantseerimisasutusele omaseid IKT- ja turvariske ning olema nendega proportsionaalsed. Ühtlasi tuleb plaani regulaarselt ajakohastada.

27. Kehtestada tuleb ametlik järelkontrolli protsess, sh sätted IKT-auditi kriitilise tähtsusega leidude ajakohaseks kinnitamiseks ja kõrvaldamiseks.

1.4. Infoturve

1.4.1. Infoturbe poliitika

28. Finantseerimisasutused peaksid töötama välja ja dokumenteerima infoturbepoliitika, milles määratletakse finantseerimisasutuste ja nende klientide andmete ning teabe konfidentsiaalsuse, andmetervikluse ja kättesaadavuse kaitsmise kõrgetasemelised põhimõtted ja eeskirjad. Makseteenuse pakkujate puhul kehtestatakse see poliitika direktiivi (EL) 2015/2366 artikli 5 lõike 1 alapunkti j alusel vastuvõetavas turvapoliitika dokumendis. Infoturbepoliitika peab olema kooskõlas finantseerimisasutuse infoturbe eesmärkidega ning põhinema riskihindamisprotsessi asjakohastel tulemustel. Vastava poliitika peaks heaks kiitma juhtorgan.

29. Poliitika peaks sisaldama infoturbehalduse peamiste rollide ja vastutuse kirjeldust ning see peaks kehtestama nõuded töötajatele ja töövõtjatele, protsessidele ja tehnoloogiale seoses infoturbega, pidades silmas, et kõigi taseme töötajatel ja töövõtjatel on kohustus tagada finantseerimisasutuse infoturvet. Poliitikas tuleb tagada finantseerimisasutuse kriitilise tähtsusega loogiliste ja füüsiliste varade, vahendite ja tundlike andmete konfidentsiaalsus, terviklus ja käideldavus nii nende säilitamisel, edastamisel kui ka kasutamisel. Infoturbe poliitika tuleb edastada kõigile finantseerimisasutuse töötajatele ja töövõtjatele.

30. Finantseerimisasutused peaksid infoturbe poliitika põhjal kehtestama turvameetmed ja neid rakendama, et leevendada IKT- ja turvariske, millele nad haavatavad on. Meetmed peaksid hõlmama järgmist:

    a) organisatsiooni ja juhtimist vastavalt punktidele 10 ja 11;
    b) loogilist turvalisust (jagu 1.4.2);
    c) füüsilist turvalisust (jagu 1.4.3);
    d) IKT-operatsioonide turvalisust (jagu 1.4.4);
    e) turvalisuse seiret (jagu 1.4.5);
    f) infoturbe ülevaatusi, hindamist ja testimist (jagu 1.4.6);
    g) infoturbealast koolitust ja teadlikkust (jagu 1.4.7).

1.4.2. Loogiline turvalisus

31. Finantseerimisasutused peaksid määrama kindlaks ja dokumenteerima loogilise juurdepääsukontrolli protseduurid (identiteedi ja juurdepääsu haldus) ning neid rakendama. Neid protseduure tuleb rakendada, jõustada, jälgida ja regulaarselt üle vaadata. Protseduurid peaksid sisaldama ka kontrolle anomaaliate seireks. Neis protseduurides tuleks minimaalselt rakendada järgmisi elemente, kus mõiste ’kasutaja’ hõlmab ka tehnilisi kasutajaid:

(a) **teadmisvajadus, minimaalõigused ja kohustuste lahusus**: finantseerimisasutused peaksid piirama infovaradele ja nende tugisüsteemidele juurdepääsu õigusi „teadmisvajaduse“ põhimõtet kasutades, sh kaugjuurdepääsu puhul. Kasutajatele tuleb anda tööülesannete täitmiseks rangelt vajalikud minimaalsed juurdepääsuõigused (minimaalõiguste printsiip), et ennetada põhjendamatut juurdepääsu suurele hulgale andmetele või ennetada selliste juurdepääsuõiguste kombinatsiooni määramist, mida võidakse kasutada kontrollidest hoidumiseks („kohustuste lahususe“ põhimõte);

(b) **kasutaja vastutus**: finantseerimisasutused peaksid võimalikult suurel määral piirama üldiste ja jagatud kasutajakontode tarvitamist ning tagama, et kasutajaid saab IKT-süsteemides tehtavates toimingutes tuvastada;

(c) **privilegeeritud juurdepääsuõigused**: finantseerimisasutused peaksid rakendama süsteemi privilegeeritud juurdepääsule tugevaid kontrolle, piirates rangelt suurema süsteemile juurdepääsuõigusega kontosid (nt administraatori kontod) ja jälgides neid hoolikalt. Turvalise side tagamiseks ja riski vähendamiseks tuleks halduslik kaugjuurdepääs kriitilise tähtsusega IKT-süsteemidele anda ainult teadmisvajaduse põhjal ja tugevate autentimislahenduste kasutamisel;

(d) **kasutaja toimingute logimine**: kõiki privilegeeritud kasutajate toiminguid tuleb vähemalt logida ja jälgida. Juurdepääsulogisid tuleb kaitsta volitamata muutmise või kustutamise eest ja nende säilitusaeg peaks olenema tuvastatud äritoimingute, tugiprotsesside ja infovarade kriitilisusest, kooskõlas jaoga 1.3.3, ilma et see piiraks Euroopa Liidu ja riiklikus õiguses sätestatud säilitamisnõuete kohaldamist. Finantseerimisasutused peaksid seda teavet kasutama teenuse osutamisel avastatud anomaalsete tegevuste tuvastamisel ja uurimisel;

(e) **juurdepääsu haldus**: juurdepääsuõigusi tuleb anda, ära võtta või muuta ajakohaselt vastavalt eelnevalt kindlaks määratud töövoogudele, mis sisaldavad asjakohase infovara omaniku kooskõlastust. Töösuhte lõpetamisel tuleb juurdepääsuõigused otsekohe eemaldada;

(f) **juurdepääsu taassertifitseerimine:** juurdepääsuõigusi tuleb regulaarselt üle vaadata, veendumaks, et kasutajatel ei ole liigseid privileege ja et juurdepääsuõigused eemaldatakse, kui neid enam vaja ei ole;

(g) **autentimismeetodid**: finantseerimisasutused peaksid kasutama piisavalt tugevaid autentimismeetodeid, mis võimaldavad küllaldaselt ja tõhusalt tagada juurdepääsukontrolli poliitikatest ja protseduuridest kinnipidamise. Autentimismeetodid peaksid vastama juurdepääsetavate IKT-süsteemide, -teabe või -protsessi kriitilisusele. Need peaksid lähtuvalt asjakohasest riskist minimaalselt sisaldama keerulisi paroole või tugevamaid autentimismeetodeid (näiteks kaheastmeline autentimine).

32. Rakenduste elektrooniline juurdepääs andmetele ja IKT-süsteemidele peaks olema piiratud miinimumini, mida on vaja asjakohase teenuse osutamiseks.

1.4.3. Füüsiline turvalisus

33. Tuleb määratleda ja dokumenteerida finantseerimisasutuste füüsilise turvalisuse meetmed ja neid rakendada, et kaitsta asutuste ruume, andmekeskusi ja tundlikke piirkondi volitamata juurdepääsu ja keskkonnaohtude eest.

34. Füüsiline juurdepääs IKT-süsteemidele peaks olema lubatud ainult volitatud isikutele. Volitused peaksid olema antud vastavalt isiku ülesannetele ja kohustustele ning piirnema isikutega, kellel on asjakohane väljaõpe ja kelle üle on tagatud seire. Füüsilist juurdepääsu tuleb regulaarselt üle vaadata, tagamaks, et ebavajalikud juurdepääsuõigused tühistatakse kohe, kui neid enam ei vajata.

35. Keskkonnaohtude eest kaitsmiseks võetud asjakohased meetmed peaksid vastama hoonete olulisusele ning nendes hoonetes asuvate operatsioonide või IKT-süsteemide kriitilisusele.

1.4.4. IKT-operatsioonide turvalisus

36. Finantseerimisasutused peaksid rakendama protseduure, millega ennetada turvaprobleemide esinemist IKT-süsteemides ja IKT-teenustes ning minimeerima nende mõju IKT-teenuse osutamisele. Need protseduurid peaksid hõlmama järgmisi meetmeid:

    a) tuvastatakse võimalikud nõrkused, mida tuleb hinnata ja parandada, tagades, et tarkvara ja püsivara on ajakohased (sh tarkvara, mille finantseerimisasutus annab oma sisestele ja välistele kasutajatele), juurutades kriitilised turbepaigad või rakendades kompenseerivaid kontrolle;
    b) rakendatakse kõigi võrgukomponentide turvalisi etalonkonfiguratsioone;
    c) rakendatakse võrgu segmenteerimist, andmekao ennetussüsteeme ja võrguliikluse krüpteerimist (vastavalt andmete liigitamisega);
    d) rakendatakse lõppseadmete, sh serverite, töökohtade ja mobiilseadmete turvet; finantseerimisasutused peaksid hindama, kas lõppseadmed vastavad nende määratletud turvastandarditele enne, kui neile ettevõtte võrgule juurdepääs antakse;
    e) tagatakse tarkvara, püsivara ja andmete terviklust kinnitavate mehhanismide olemasolu;
    f) krüpteeritakse andmed nii säilitamisel kui edastamisel (vastavalt andmete liigitusega).

37. Finantseerimisasutused peaksid lisaks pidevalt jälgima, kas nende tegevuskeskkonna muutused mõjutavad olemasolevaid turvameetmeid või on kaasneva riski maandamiseks vaja täiendavaid meetmeid. Need muutused peaksid olema osa finantseerimisasutuse ametlikust muudatuste halduse menetlusest, millega tagatakse, et kõiki muudatusi kavandatakse, testitakse, dokumenteeritakse, volitatakse ja võetakse kasutusele nõuetekohaselt.

1.4.5. Turvaseire

38. Finantseerimisasutused peaksid kehtestama ja rakendama poliitikaid ja protseduure, millega tuvastada ebaharilikke toiminguid, mis võivad mõjutada finantseerimisasutuse infoturvet, ja neile sündmustele nõuetekohaselt reageerima. Pideva seire osana peaksid finantseerimisasutused rakendama asjakohast ja efektiivset võimekust tuvastada füüsilist või

loogilist sissetungi ning infovarade konfidentsiaalsuse, tervikluse ja käideldavuse rikkumisi, ning neist teavitama. Pideva seire ja tuvastuse protsessid peaksid hõlmama:

a) asjakohaseid sise- ja välistegureid, sealhulgas äri- ja IKT-haldustoiminguid;
b) toiminguid, millega tuvastada kolmandate isikute või teiste üksuste juurdepääsu väärkasutust ja asutusesisest juurdepääsu väärkasutust;
c) võimalikke sise- ja välisohte.

39. Finantseerimisasutused peaksid kehtestama ja rakendama protsesse ja organisatsioonilisi struktuure, et tuvastada ja pidevalt jälgida turvaohte, mis võivad oluliselt kahjustada nende võimet teenuseid pakkuda. Finantseerimisasutused peaksid aktiivselt jälgima tehnoloogia arengut ja tagama, et nad teadvustavad turvariske. Finantseerimisasutused peaksid rakendama tuvastusmeetmeid, näiteks selleks, et tuvastada võimalikud infolekked, ründekoodi ja muud turvaohud, avalikult teada olevad tarkvara ja riistvara nõrkused, ning kontrollima vastavate uute turvauuenduste olemasolu.

40. Turvaseire protsess peaks ka aitama finantseerimisasutusel mõista operatsiooni- või turvaintsidentide olemust, tuvastada trende ja toetada organisatsiooni uurimisi.

1.4.6. Infoturbe ülevaated, hindamine ja testimine

41. Finantseerimisasutused peaksid tegema erinevaid infoturbe ülevaatuseid, hindamisi ja testimisi, et tagada oma IKT-süsteemide ja IKT-teenuste nõrkuste tõhusat tuvastamist. Finantseerimisasutused võivad näiteks teostada lahknevusanalüüsi võrreldes infoturbe standarditega, vastavusülevaateid, infosüsteemide siseseid ja väliseid auditeid või füüsilise turvalisuse kontrolle. Lisaks peaks asutus kaaluma selliseid häid tavasid nagu lähtekoodi ülevaatused, nõrkuste hindamised, läbistustestid ja punase tiimi harjutused.

42. Finantseerimisasutused peaksid kehtestama ja rakendama infoturbe testimise raamistikku, millega kinnitatakse nende infoturbemeetmete tugevust ja tõhusust, ning veenduma, et selles raamistikus arvestatakse ohtude seire ning IKT- ja turvariskide hindamise protsessi käigus tuvastatud ohtude ja nõrkustega.

43. Infoturbe testimisraamistik peaks tagama, et

a) teste teevad sõltumatud testijad, kellel on infoturbemeetmete testimise vallas piisavalt teadmisi, oskusi ja kogemust ning kes ei osalenud infoturbemeetmete väljatöötamises;
b) testid hõlmavad nõrkuste analüüse ja läbistusteste (sh vajadusel ja sobivusel ohust lähtuvaid läbistusteste), mis vastavad äriprotsesside ja süsteemidega tuvastatud riskitasemele.

44. Finantseerimisasutused peaksid turvameetmeid pidevalt ja korduvalt testima. Kõigi kriitiliste IKT-süsteemide (lõige 17) puhul tuleks neid teste teha vähemalt kord aastas ning makseteenuste pakkujate puhul kuuluvad testid nende osutatavate makseteenustega seotud turvariskide põhjaliku hindamise alla vastavalt teise makseteenuste direktiivi artikli 95 lõikele 2. Mittekriitilisi süsteeme tuleks testida regulaarselt ja riskipõhiselt, kuid vähemalt kord kolme aasta jooksul.

45. Finantseerimisasutused peaksid tagama, et turvameetmete teste tehakse taristu, protsesside või protseduuride muudatuste korral ja kui muudatusi tehakse oluliste operatsiooni- või turvaintsidentide tõttu või uute/märkimisväärselt muudetud välisvõrguga suhtlevate kriitiliste rakenduste avaldamisel.

46. Finantseerimisasutused peaksid jälgima ja hindama turvatestide tulemusi ning ajakohastama nende alusel turvameetmeid, kriitilise tähtsusega IKT-süsteemide korral ilma liigsete viivitusteta.

47. Makseteenuse pakkujate puhul peaks testimisraamistik hõlmama ka järgmiste vahendite turvameetmeid: (1) makseterminalid ja -seadmed, mida kasutatakse makseteenuse pakkumiseks (2) makseteenuse kasutaja autentimiseks kasutatavad makseterminalid ja -seadmed ning (3) makseteenuse kasutajale autentimiskoodi genereerimiseks/saamiseks antavad seadmed ja tarkvara.

48. Leitud turvaohtude ja tehtud muudatuste põhjal tuleks teha testimine, milles kasutatakse ka asjakohaste ja teada olevate potentsiaalsete rünnete stsenaariume.

1.4.7. Infoturbekoolitus ja sellealane teadlikkus

49. Finantseerimisasutused peaksid kehtestama koolitusprogrammi, sh regulaarsed turvalisuse alase teadlikkuse programmid kõigile töötajaile ja töövõtjatele, tagamaks, et nad kõik on saanud väljaõppe oma ülesannete ja kohustuste täitmiseks vastavalt asjakohastele turvaeeskirjadele ja -protseduuridele, et vähendada inimlikke eksimusi, vargusi, pettusi, väärkasutamist või kahju ja et nad teaksid, kuidas tulla toime infoturbega seotud riskidega. Finantseerimisasutused peaksid tagama, et koolitusprogrammiga koolitatakse kõiki töötajaid ja töövõtjaid vähemalt kord aastas.

1.5. IKT-tegevuste haldus

50. Finantseerimisasutused peaksid haldama oma IKT-tegevusi dokumenteeritud ja rakendatud protsesside ja protseduuride põhjal (mis makseteenuste pakkujate puhul hõlmavad juhtorgani heaks kiidetud teise makseteenuste direktiivi artikli 5 lõike 1 alampunkti j kohast turvapoliitikadokumenti). Selles dokumentide kogumikus tuleks määrata kindlaks, kuidas finantseerimisasutused oma IKT-süsteeme käitavad, jälgivad ja kontrollivad, sh kriitilise tähtsusega IKT-tegevuste dokumenteerimine, mis võimaldaks finantseerimisasutustel hallata ajakohast IKT-varade inventuuri.

51. Finantseerimisasutused peaksid tagama, et IKT-tegevuste sooritus vastab nende äri nõuetele. Finantseerimisasutused peaksid säilitama oma IKT-tegevuste tõhusust ja seda võimalusel parandama, sealhulgas, kuid mitte ainult kaaluma, kuidas minimeerida käsitsi tehtavate ülesannete läbiviimisest tulenevaid võimalikke vigu.

52. Finantseerimisasutused peaksid rakendama kriitilise tähtsusega IKT-tegevuste osas logimist ja seiret, et võimaldada vigade tuvastamist, analüüsi ja parandamist.

53. Finantseerimisasutused peaksid haldama oma IKT-varade (sh IKT-süsteemide, võrguseadmete, andmebaaside jms) ajakohast loendit. IKT-varade loendis tuleks hoiustada IKT-varade seadistust ning erinevate IKT-varade vahelisi seoseid ja vastastikuseid sõltuvusi õige konfigureerimise ja muudatuste haldamise protsessi toimimise tagamiseks.

54. IKT-varade loend peaks olema piisavalt detailne, et võimaldada IKT-vara, selle asukohta, turvaliigitust ja kuuluvust kiirelt tuvastada. Varadevahelised vastastikused sõltuvused tuleb dokumenteerida, et toetada turva- ja operatiivsetele intsidentidele, sh küberrünnakutele reageerimist.

55. Finantseerimisasutused peaksid jälgima ja haldama IKT-varade elutsükleid, veendumaks, et need vastavad jätkuvalt äri- ja riskijuhtimise nõuetele ning toetavad neid. Finantseerimisasutused peaksid jälgima, kas nende välised ja ettevõttesisesed tarnijad ja arendajad toetavad nende IKT-varasid ning kas kõiki asjakohaseid paikasid ja värskendusi paigaldatakse dokumenteeritud protsesside kohaselt. Vananenud või ilma toeta IKT-varadest tulenevaid riske tuleb hinnata ja maandada.

56. Finantseerimisasutused peaksid rakendama jõudluse ja suutlikkuse planeerimise ning seire protsesse IKT-süsteemide oluliste sooritusprobleemide ja IKT-võimekuse puudujääkide ajakohaseks ennetamiseks ja tuvastamiseks ning nendega tegelemiseks.

57. Finantseerimisasutused peaksid määratlema ja rakendama andme- ja IKT-süsteemide varundamise ja taastamise protseduure tagamaks nende nõuetekohane taastamine. Varundamise ulatus ja sagedus tuleb sätestada vastavalt äri taastamisnõuetele ning andme- ja IKT-süsteemide kriitilisusele ning seda tuleb hinnata kooskõlas teostatud riskihindamisega. Varundamise ja taasteprotseduure tuleb regulaarselt testida.

58. Finantseerimisasutused peaksid tagama, et andme- ja IKT-süsteemi varukoopiaid hoitakse turvaliselt ning need on põhiasukohast piisavalt kaugel, et neid ei ohustaks samad riskid.

3.5.1 IKT intsidentide ja probleemide haldus

59. Finantseerimisasutused peaksid kehtestama ja rakendama intsidentide ja probleemide halduse protsessi, et jälgida ja logida operatsiooni ja turvalisusega seotud IKT-intsidente ning võimaldada katkestuste esinemisel finantseerimisasutustel kiirelt kriitiliste ärifunktsioonide ja -protsessidega jätkata. Finantseerimisasutused peaksid määratlema asjakohased kriteeriumid ja läved, et liigitada sündmused operatsiooni- või turvaintsidendiks, nagu on sätestatud suuniste mõistete osas, samuti eelhoiatuse indikaatorid, mis peaksid toimima hoiatusteatena, et neid intsidente saaks aegsasti tuvastada. Need makseteenuse pakkujate kriteeriumid ja läved ei piira teise makseteenuste direktiivi artikli 96 alusel suurte intsidentide liigitamist ja teise makseteenuste direktiivi kohaseid suurtest intsidentidest teavitamise suuniseid (EBA/GL/2017/10).

60. Kahjulike sündmuste mõju minimeerimiseks ja kiire taastumise võimaldamiseks peaksid finantseerimisasutused kehtestama nõuetekohased protsessid ja organisatsioonilised struktuurid, mis tagavad operatsiooni- ja turvaintsidentide järjepideva ning integreeritud seire, käsitlemise ja järelmeetmete rakendamise, veendumaks, et algpõhjused kõrvaldatakse korduvate intsidentide esinemise ennetamiseks. Intsidendi- ja probleemihalduse protsessis tuleks kehtestada:

    a) protseduurid intsidentide tuvastamiseks, jälgimiseks, logimiseks, liigitamiseks ja prioriteetsuse alusel klassifitseerimiseks, lähtudes äri kriitilisusest;
    b) rollid ja kohustused erinevate intsidentide stsenaariumite jaoks (nt vead, talitlushäired, küberrünnakud);
    c) probleemihalduse protseduurid ühe või enama intsidendi algpõhjuse tuvastamiseks, analüüsimiseks ja lahendamiseks – finantseerimisasutus peaks analüüsima finantseerimisasutust potentsiaalselt mõjutavaid operatsiooni- ja turvaintsidente, mis on tuvastatud või esinenud ettevõttes ja/või sellest väljaspool, võtma arvesse nendest analüüsidest saadud peamisi õppetunde ning turvameetmeid vastavalt ajakohastama;
    d) tõhusad ettevõttesisesed kommunikatsiooniplaanid, sh intsidentidest teavitamine ja eskalatsioonimenetlused – mis hõlmavad ka klientidelt saabuvaid turvalisusega seotud kaebusi – tagamaks, et:
        i) kõrgemat juhtkonda ja IKT kõrgemat juhtkonda teavitatakse kriitilise tähtsusega IKT-süsteemidele ja IKT-teenustele potentsiaalselt väga halba mõju avaldavatest intsidentidest;
        ii) juhtorganit hoitakse vastavalt vajadusele kursis märkimisväärsete intsidentidega ning teavitatakse vähemalt selle mõjust, reageerimisest ja intsidendi tulemusena tuvastatud täiendavate meetmete vajalikkusest;
    e) intsidentidele reageerimise protseduurid, millega leevendatakse intsidentidega seotud mõju ja tagatakse, et teenus on õigeaegselt kasutatav ja turvaline;
    f) konkreetsed väliskommunikatsiooniplaanid kriitiliste ärifunktsioonide ja protsesside jaoks, et:
        i) teha intsidendile tõhusalt reageerimisel ja sellest taastumisel koostööd asjakohaste sidusrühmadega;
        ii) anda välistele pooltele (nt klientidele, teistele turuosalistele, järelevalveasutusele) ajakohast teavet, mis on kohaldatava regulatsiooni seisukohast nõuetekohane ja sellega kooskõlas.

1.6. IKT-projekti ja muudatuste haldus

1.6.1. IKT-projekti haldus

61. Finantseerimisasutus peaks kehtestama programmi ja/või projektijuhtimise protsessi, kus on määratletud rollid, kohustused ja aruandekohuslused, et IKT-strateegia elluviimist tõhusalt toetada.

62. Finantseerimisasutus peaks nõuetekohaselt jälgima ja leevendama oma IKT-projektide portfellist tulenevaid riske (programmi juhtimine), arvestades ühtlasi riskidega, mis võivad tuleneda erinevate projektide omavahelistest seostest ja samade ressursside ja/või oskusteabe põhiste projektide sõltuvustest.

63. Finantseerimisasutus peaks kehtestama ja rakendama IKT-projektijuhtimise põhimõtted, mis sisaldavad vähemalt:

    a) projekti eesmärke;
    b) rolle ja kohustusi;
    c) projekti riskihindamist;
    d) projekti plaani, ajakava ja etappe;
    e) peamisi vahe-eesmärke;
    f) muudatuste juhtimise nõudeid.

64. IKT-projektijuhtimise põhimõtetes tuleb tagada, et infoturbe nõudeid analüüsib ja kiidab heaks arendamisfunktsioonist sõltumatu funktsioon.

65. Finantseerimisasutus peaks tagama, et projekti töörühmas on esindatud kõik IKT-projektist mõjutatud valdkonnad ning et projekti töörühmal on vajalikud teadmised projekti turvalise ja eduka elluviimise tagamiseks.

66. Juhtorganit tuleb regulaarselt ja vajadusel sagedamini teavitada IKT-projektide alustamisest ning edenemisest ning nendega seotud riskidest kas eraldi või koondatult sõltuvalt IKT-projektide olulisusest ja suurusest. Finantseerimisasutused peaksid projekti riski oma riskijuhtimise raamistikku kaasama.

1.6.2. IKT-süsteemide soetamine ja arendamine

67. Finantseerimisasutused peaksid välja töötama ja rakendama IKT-süsteemide soetamist, arendamist ja hooldust reguleeriva protsessi. Protsessi kavandamisel tuleb lähtuda riskipõhisest lähenemisest.

68. Finantseerimisasutus peaks tagama, et enne IKT-süsteemide soetamist või arendamist on ettevõtte asjakohane juhtkond funktsionaalsed ja mittefunktsionaalsed nõuded (sh infoturbe nõuded) selgelt määratlenud ja heaks kiitnud.

69. Finantseerimisasutus peaks tagama meetmete olemasolu, et maandada IKT-süsteemide tahtmatute muudatuste või tahtlike manipulatsioonide riski arendamise ajal ning juurutamisel tootmiskeskkonda.

70. Finantseerimisasutustel peaks olema kehtestatud metoodika IKT-süsteemide testimiseks ja heaks kiitmiseks enne esimest kasutamist. Selles metoodikas tuleks arvestada äriprotsesside ja varade kriitilisusega. Testimise käigus tuleb tagada, et uued IKT-süsteemid toimivad kavandatud viisil. Ühtlasi tuleks kasutada testimiskeskkondi, mis tootmiskeskkonda adekvaatselt kajastavad.

71. Finantseerimisasutused peaksid testima IKT-süsteeme, IKT-teenuseid ja infoturbe meetmeid, et tuvastada võimalikud turvalisuse puudujäägid, rikkumised ja intsidendid.

72. Finantseerimisasutus peaks kasutama eraldi IKT-keskkondi, et tagada piisav kohustuste lahusus ja maandada kontrollimata muudatuste mõju tootmissüsteemidele. Täpsemalt peaks finantseerimisasutus tagama tootmiskeskkondade lahutamise arendus-, test- ja muudest tootmisega mitteseotud keskkondadest. Finantseerimisasutus peaks tagama tootmisandmete tervikluse ja konfidentsiaalsuse tootmisega mitteseotud keskkondades. Ainult volitatud kasutajad võivad tootmisandmetele ligi pääseda.

73. Finantseerimisasutused peaksid võtma meetmeid, et kaitsta ettevõttes arendatavate IKT-süsteemide lähtekoode. Lisaks peaksid nad igakülgselt dokumenteerima IKT-süsteemide arendamist, rakendamist, käitamist ja/või seadistamist, et ei oleks vaja liigselt sõltuda vastava valdkonna ekspertidest. IKT-süsteemi dokumentatsioon peaks kohaldatavatel juhtudel sisaldama vähemalt kasutaja dokumentatsiooni, tehnilise süsteemi dokumentatsiooni ja käitusprotseduure.

74. 74. Finantsinstitutsiooni IKT-süsteemide omandamise ja arendamise protsesse tuleks kohaldada ka IKT-süsteemide suhtes, mille on välja töötanud või haldavad ärifunktsiooni lõppkasutajad väljaspool IKT-organisatsiooni (nt lõpptarbija andmetöötlusrakendused) riskipõhist lähenemisviisi kasutades. Finantseerimisasutus peaks pidama kriitilise tähtsusega ärifunktsioone või protsesse toetavate rakenduste registrit.

1.6.3. IKT muudatuste haldus

75. Finantseerimisasutused peaksid kehtestama ja rakendama IKT muudatuste halduse protsessi, et tagada kõigi IKT-süsteemide muudatuste registreerimine, testimine, hindamine, kinnitamine, rakendamine ja tõendamine kontrollitud viisil. Finantseerimisasutused peaksid eriolukordades (nt muudatused, mida tuleb rakendada niipea kui võimalik) tegelema muudatustega piisavaid kaitsemeetmeid tagavate protseduuride alusel.

76. Finantseerimisasutused peaksid pidevalt jälgima, kas muudatused olemasolevas tegevuskeskkonnas mõjutavad olemasolevaid turvameetmeid või on kaasnevate riskide maandamiseks vaja võtta täiendavaid meetmeid. Need muudatused peaksid olema vastavuses finantseerimisasutuste ametliku muutuste haldamise protsessiga.

1.7. Talitluspidevuse korraldamine

77. Finantseerimisasutused peaksid kehtestama usaldusväärse talitluspidevuse juhtimise protsessi, mis maksimeeriks nende võimet järjepidevalt teenuseid osutada ja vähendaks äritegevuse tõsise häire korral kahjusid kooskõlas direktiivi (EL) 2013/36 artikli 85 lõikega 2 ja EBA sisemise juhtimissüsteemi suuniste jaotisega VI (EBA/GL/2017/11).

1.7.1. Ärimõju analüüs

78. Osana talitluspidevuse planeerimisest peaksid finantseerimisasutused läbi viima ärimõju analüüsi, analüüsides oma riskipositsiooni äritegevuse tõsiste häirete korral ja hinnates nende võimalikku mõju (sh konfidentsiaalsusele, andmeterviklusele ja käideldavusele) nii kvalitatiivselt kui kvantitatiivselt, kasutades sisemisi ja/või väliseid andmeid (nt äriprotsessi seisukohast asjakohaseid kolmandast isikust teenuseosutaja andmeid või avalikult kättesaadavaid andmeid, mis võivad ärimõju hinnangu jaoks asjakohased olla) ja tegema stsenaariumianalüüsi. Ärimõju analüüsis tuleks arvestada ka tuvastatud ja liigitatud ärifunktsioonide, tugiprotsesside, kolmandate isikute ja infovarade kriitilisuse ning nende omavaheliste seostega kooskõlas jaoga 1.3.3.

79. Finantseerimisasutused peaksid tagama, et nende IKT-süsteemid ja IKT-teenused on kavandatud ja kooskõlas ärimõju analüüsiga, näiteks teatud kriitilise tähtsusega komponentide liiasus, et ennetada katkestusi, mida võivad põhjustada neid komponente mõjutavad sündmused.

1.7.2. Talitluspidevuse planeerimine

80. Finantseerimisasutused peaksid ärimõju analüüsi alusel koostama talitluspidevuse tagamise kavad (talitluspidevuse plaanid), mis tuleks dokumenteerida ja heaks kiita nende juhtorganites. Nendes plaanides tuleb konkreetselt arvestada riskidega, mis võivad IKT-süsteeme ja IKT-teenuseid kahjulikult mõjutada. Plaanid peaksid toetama eesmärke kaitsta ja vajaduse korral taastada oma ärifunktsioonide, tugiprotsesside ja infovarade konfidentsiaalsus, terviklus ning käideldavus. Finantseerimisasutused peaksid vajadusel plaane nende koostamisel asjakohaste siseste ja väliste sidusrühmadega kooskõlastama.

81. Finantseerimisasutused peaksid kehtestama talitluspidevuse plaanid, et tagada asjakohane reageerimine võimalikele rikkestsenaariumitele ja olla võimelised taastama oma kriitilise tähtsusega äritoimingute töö pärast katkestusi taasteaja eesmärgi (maksimaalne aeg, mille jooksul süsteem või protsess tuleb pärast intsidenti taastada) ja taaste sihtseisu (maksimaalne ajavahemik, mille jooksul on intsidendi korral andmekadu vastuvõetav) piires. Konkreetseid talitluspidevuse plaane käivitavate äritegevuse tõsiste häirete puhul peaksid finantseerimisasutused lähtuma talitluspidevuse toimingute prioriteetide seadmisel riskipõhisest lähenemisest, mis võib tugineda jao 1.3.3 kohaselt läbi viidavatele riskihindamistele. Makseteenuste pakkujate puhul võib see hõlmata näiteks kriitilise tähtsusega tehingute edasise töötlemise toetamist samal ajal kui jätkatakse leevendusmeetmetega.

82. Finantseerimisasutus peaks oma talitluspidevuse plaanis arvestama paljusid erinevaid stsenaariume, sealhulgas äärmuslikke, kuid usutavaid stsenaariume, millega ta võib kokku puutuda (sealhulgas küberrünnaku stsenaarium) ning hindama nende võimalikku mõju. Nende stsenaariumite põhjal peaks finantseerimisasutus kirjeldama, kuidas tagatakse IKT-süsteemide ja -teenuste ning finantseerimisasutuse infoturbe talitluspidevus.

1.7.3. Reageerimis- ja taasteplaanid

83. Finantseerimisasutused peaksid ärimõju analüüside (lõige 78) ja usutavate stsenaariumite (lõige 82) alusel reageerimis- ja taasteplaanid välja töötama. Nendes plaanides tuleb täpsustada, millistel tingimustel plaanid käivitatakse ning milliseid meetmeid tuleb võtta, et tagada vähemalt finantseerimisasutuse kriitilise tähtsusega IKT-süsteemide ja IKT-teenuste käideldavus, talitluspidevus ja taastamine. Reageerimis- ja taasteplaanide eesmärk peaks olema finantseerimisasutuse tegevuste taaste-eesmärkide täitmine.

84. Reageerimis- ja taasteplaanides tuleks arvestada nii lühi- kui ka pikaajaliste taastetegevustega. Plaanid:

    a) peaksid keskenduma kriitilise tähtsusega ärifunktsioonide, tugiprotsesside, infovarade ja nendevaheliste seoste taastamisele, et vältida kahjulikku mõju finantseerimisasutuse ja finantssüsteemi toimimisele, sh maksesüsteemidele ja makseteenuse kasutajatele, ning tagada ootel olevate maksetehingute täideviimine;
    b) tuleks dokumenteerida ning teha äri- ja tugiüksustele teatavaks ja hädaolukorras kergesti kättesaadavaks; ning
    c) tuleks ajakohastada intsidentide, testide, uute tuvastatud riskide ja ohtude põhjal saadud kogemuste ning muudetud taastamiseesmärkide ja prioriteetide alusel.

85. Plaanides tuleks arvestada ka alternatiivsete võimalustega, kus taastamine pole kulude, riskide, logistika või ettenägematute asjaolude tõttu lühemas plaanis saavutatav.

86. Lisaks peaks finantseerimisasutus osana reageerimis- ja taasteplaanidest kaaluma ja rakendama talitluspidevuse meetmeid finantseerimisasutuse IKT-teenuse talitluspidevuse seisukohast olulise tähtsusega kolmandast isikust teenuseosutajate tõrgete leevendamiseks (kooskõlas EBA suunistega tegevuse edasiandmise kokkulepete alal (EBA/GL/2019/02) seoses talitluspidevuse plaanidega).

1.7.4. Plaanide testimine

87. Finantseerimisasutused peaksid oma talitluspidevuse plaane regulaarselt testima. Täpsemalt peaksid nad tagama oma kriitilise tähtsusega ärifunktsioonide, tugiprotsesside, infovarade ja nendevaheliste seoste (sh vajadusel kolmandate isikute osutatavate teenuste) testimise vähemalt kord aastas kooskõlas lõikega 89.

88. Talitluspidevuse plaane tuleks ajakohastada vähemalt kord aastas, tuginedes testimistulemustele, olemasolevatele ohtude andmetele ja varasematest sündmustest saadud kogemustele. Mis tahes muudatusi taaste-eesmärkides (sealhulgas taasteaja eesmärk ja taaste sihtseis) ja/või muutusi ärifunktsioonides, tugiprotsessides ja infovarades tuleks vajaduse korral kaaluda ka talitluspidevuse plaanide ajakohastamise alusena.

89. Finantseerimisasutuste tehtavad talitluspidevuse plaanide testid peaksid näitama, et asutused suudavad oma äride elujõulisust kuni kriitiliste tegevuste ennistamiseni alal hoida. Eelkõige peaks:

a) testimisse kaasama tõsiseid, ent usutavaid stsenaariume, sh neid, mida kaalutakse talitluspidevuse plaanide välja töötamiseks (ning vajadusel testima kolmandate isikute osutatavaid teenuseid); selle käigus tuleks kriitilise tähtsusega ärifunktsioonid, tugiprotsessid ja infovarad lülitada ümber nende avariijärgse taaste keskkonda ja näidata, et need suudavad sellisel viisil piisavalt pika ajavahemiku vältel töötada ning et hiljem on normaalse toimimise taastamine võimalik;
b) olema ette nähtud kontrollima talitluspidevuse plaanide aluseeldusi, sealhulgas juhtimiskorraldust ja kriisikommunikatsiooni plaane; ning
c) hõlmama protseduure töötajate, töövõtjate, IKT-süsteemide ja IKT-teenuste võimekuse kontrollimiseks, et lõike 89 punktis a määratletud stsenaariumitele adekvaatselt reageerida.

90. Testi tulemusi tuleb dokumenteerida ning testidest tulenevaid tuvastatud puudujääke tuleb analüüsida, nendega tegeleda ja juhtorganit neist teavitada.

1.7.5. Kriisikommunikatsioon

91. Tegevuste katkestuse korral või hädaolukorras ning talitluspidevuse plaanide rakendamisel peaksid finantseerimisasutused tagama, et neil on olemas tõhusad kriisikommunikatsioonimeetmed, et kõik sisesed ja välised sidusrühmad, sealhulgas regulatsioonides nõutud juhtudel pädevad asutused, ning asjaomased teenuseosutajad (allhanke teenuseosutajad, kontserni üksused või kolmandast isikust teenuseosutajad) saaksid teavet õigeaegselt ja asjakohasel viisil.

1.8. Makseteenuse kasutajate suhtehaldus

92. Makseteenuse pakkujad peaksid kehtestama ja rakendama protsessid, millega teadvustatakse makseteenuse kasutajatele makseteenuste turvariske, pakkudes makseteenuse kasutajatele abi ja suuniseid.

93. Makseteenuse kasutajatele pakutavad abi ja suunised tuleks uute ohtude ja nõrkuste suhtes ajakohastada ning muudatustest tuleks makseteenuse kasutajat teavitada.

94. Kui toote funktsionaalsus võimaldab, peaksid makseteenuse pakkujad võimaldama makseteenuse kasutajatel välja lülitada teatud maksetoiminguid, mis on seotud makseteenuse pakkuja poolt makseteenuse kasutajale pakutavate makseteenustega.

95. Kui makseteenuse pakkuja on direktiivi (EL) 2015/2366 artikli 68 lõike 1 kohaselt nõustunud maksja kulutuste limiidiga konkreetsete makseinstrumentide kaudu täidetavate maksetehingute korral, peaks ta andma maksjale võimaluse suurendada limiite kuni maksimaalse kokkulepitud limiidini.

96. Makseteenuse pakkujad peaksid pakkuma makseteenuse kasutajale võimalust saada hoiatusteateid maksetehingute alustamise ja/või ebaõnnestunud alustamiskatsete kohta, et nad saaksid tuvastada oma kontode petturlikku või pahatahtlikku kasutamist.

97. Makseteenuse pakkujad peaksid teatama makseteenuse kasutajaile selliste turvaprotseduuride uuendustest, mis mõjutavad makseteenuse kasutajaid seoses makseteenuse pakkumisega.

98. Makseteenuse pakkujad peaksid andma makseteenuse kasutajatele abi kõigi makseteenustega seonduvate küsimuste, abipalvete ja anomaaliateadete või turvaprobleemide korral. Makseteenuse kasutajaid tuleks asjakohaselt teavitada, kuidas sellist abi saada.