Finantsinspektsioon

# TIBER-EE riiklik rakendusjuhend

Käesolev juhend kirjeldab TIBER-EE raamistiku rakendamist Eestis

2026

Finantsinspektsioon

FINANTSINSPEKTSIOONI
SOOVITUSLIK JUHEND

Tallinn

# TIBER-EE riiklik rakendusdokument

Soovituslik juhend on kehtestatud Finantsinspektsiooni juhatuse 15.09.2026 otsusega nr 1.1-7/143 Finantsinspektsiooni seaduse § 57 lõike 1 ja lõike 3 alusel.

# Sisukord

# 1. Üldsätted

## 1.1. Pädevus

1.1.1. Finantsinspektsiooni seaduse (edaspidi FIS) § 3 lõike 1 kohaselt teostab Finantsinspektsioon riiklikku finantsjärelevalvet finantssektori stabiilsuse, usaldusväärsuse ja läbipaistvuse ning toimimise efektiivsuse suurendamise, süsteemsete riskide vähendamise ning finantssektori kuritegelikel eesmärkidel ärakasutamise tõkestamisele kaasaaitamise eesmärgil, et kaitsta klientide ja investorite huve nende vahendite säilimisel ning seeläbi toetada Eesti rahasüsteemi stabiilsust.

1.1.2. FIS § 57 lõike 1 kohaselt on Finantsinspektsioonil õigus välja anda soovitusliku iseloomuga juhendeid finantssektori tegevust reguleerivate õigusaktide selgitamiseks või finantsjärelevalve subjektide suunamiseks.

## 1.2. Eesmärk ja kohaldamisala

1.2.1. Käesolev juhend (edaspidi *juhend*) on ohuteabel põhineva eetilise punase meeskonna testimise Euroopa raamistiku (Threat Intelligence-Based Ethical Red Teaming, edaspidi *TIBER-EU*) riiklik rakendusdokument Eestis. Juhendis kirjeldatud TIBER-EU raamistiku riiklikku rakendust nimetatakse TIBER-EE-ks. Juhend selgitab TIBER-EE kasutamist ohuteabel põhineva läbistustestimise (Threat-Led Penetration Testing, edaspidi *TLPT*) eesmärgil vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2022/2554 finantssektori digitaalse tegevuskerksuse kohta (edaspidi *DORA*).

1.2.2. DORA eesmärk on tugevdada finantssektori digitaalset tegevuskerksust, kehtestades ühtsed nõuded muu hulgas IKT-riskide juhtimisele, IKT-intsidentide käsitlemisele ja raporteerimisele, digitaalse tegevuskerksuse testimisele ning kolmandatest isikutest IKT-teenuseosutajatega seotud riskide juhtimisele. DORA kohaldub määruse artiklis 2 nimetatud finantssektori ettevõtjatele, arvestades samas artiklis sätestatud erandeid. DORA artikli 26 kohaselt peavad pädeva asutuse poolt selleks tuvastatud finantssektori ettevõtjad perioodiliselt läbi viima TLPT-d.

1.2.3. Eestis on Finantsinspektsioon DORA kohaselt pädev asutus oma järelevalvepädevusse kuuluvate finantssektori ettevõtjate jaoks. Selles rollis ning ohuteabel põhineva läbistustestimise asutusena kohaldab Finantsinspektsioon TIBER-EE-d kui TIBER-EU raamistiku riiklikku rakendust TLPT testimiste

läbiviimiseks Finantsinspektsiooni TLPT pädevusse kuuluvate finantssektori ettevõtjate suhtes.

1.2.4. TIBER tähendab ohuteabel põhinevat eetilist punase meeskonna testimist. Tegemist on raamistikuga, mille alusel viiakse tootmiskeskkondades läbi kontrollitud ja ohuteabel põhinevaid teste kriitiliste või oluliste funktsioonide ja neid toetavate süsteemide suhtes eesmärgiga tugevdada testitava üksuse küberkerksust ja tegevusvalmidust.

1.2.5. TIBER-EE-d tuleks mõista kui tegevuskerksust tugevdavat ja õppimisele suunatud raamistikku. See ei ole mõeldud läbimise või läbikukkumise testina, vaid struktureeritud ja kontrollitud vahendina, mis aitab finantssektori ettevõtjatel tuvastada oma kaitse-, avastamis- ja reageerimisvõime tugevusi, nõrkusi ning parendusvajadusi, tagades samal ajal, et testimine toimub turvaliselt ja vastutustundlikult.

1.2.6. Käesolevat juhendit tuleks lugeda koos TIBER-EU raamistiku ja Euroopa Keskpanga (edaspidi EKP) välja antud seotud suunistega[1] ning DORA alusel vastu võetud TLPT regulatiivsete tehniliste standarditega (edaspidi *RTS*) (komisjoni delegeeritud määrus (EL) 2025/1190)[2].

1.2.7. Finantsinspektsioon võib esitada või osutada täiendavatele viidetele, mallidele või kontaktpunktidele, mis on asjakohased TIBER-EE kohaldamiseks Eestis.

1.2.8. Kõik TIBER-EU raamistiku kohustuslikud nõuded kohalduvad vahetult TIBER-EE testidele. Käesolev juhend ei dubleeri kogu TIBER-EU metoodikat, vaid sätestab Eestis kohaldatava riikliku juhtimismudeli ja eripärad. TIBER-EE on TIBER-EU raamistiku riiklik rakendus Eestis ning käesoleva juhendi kohaldamisalas kasutatav metoodiline raamistik DORA kohaste TLPT-de läbiviimiseks.

1.2.9. RTS-i kohaselt võivad finantssektori ettevõtjad, kes peavad läbi viima ohuteabel põhineva läbistustestimise, kasutada TIBER-EU raamistikku või selle riiklikku

[1] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[2] https://eur-lex.europa.eu/eli/reg_del/2025/1190/oj/eng

rakendusdokumenti, tingimusel et see on kooskõlas DORA määruse artiklite 26 ja 27 ning RTS-is sätestatud nõuetega.

1.2.10. Käesolev juhend on mõeldud:

- Eesti finantssektori ettevõtjatele, kelle Finantsinspektsioon on DORA alusel tuvastanud TLPT kohustuslastena ning kelle suhtes on tehtud vastav järelevalveline otsus;
- teistele Eesti finantssektori ettevõtjatele, kes soovivad TIBER-EE teste läbi viia vabatahtlikkuse alusel; ning
- kolmandast isikust teenuseosutajatele ja teistele puudutatud isikutele, kes osalevad TIBER-EE testides.

1.2.11. Finantssektori ettevõtjate puhul, kelle Finantsinspektsioon on tuvastanud DORA alusel TLPT kohustuslastena ning kelle suhtes on tehtud vastav järelevalveline otsus, on käesolev TIBER-EE juhend selliste testide läbiviimise riiklik raamistik. Teised finantssektori ettevõtjad võivad kasutada TIBER-EE-d vabatahtlikkuse alusel tingimusel, et see on eelnevalt Finantsinspektsiooniga kooskõlastatud.

1.2.12. TIBER-EE kohaldub Eesti finantssektoris käesolevas juhendis sätestatud ulatuses, arvestades punktis 4.5 sätestatud erisusi. Teised sektorid võivad kasutada TIBER-EU raamistikku vabatahtlikkuse alusel, kuid sellised testid jäävad väljapoole käesoleva juhendi kohaldamisala ning väljapoole Finantsinspektsiooni hallatavaid TIBER-EE juhtimiskorraldusi.

## 1.3. Õiguslik märkus

1.3.1. Käesolev juhend kirjeldab TIBER-EU raamistiku rakendamist Eestis ning on mõeldud soovitusliku juhendina. Juhendi näol ei ole tegemist õigusnõuga, samuti ei asenda see kohaldatavaid õigusakte ega siduvaid regulatiivseid nõudeid ning seda tuleb lugeda koos kohaldatava õigusliku ja regulatiivse raamistikuga.

1.3.2. Juhendi kohaldamisel tuleb arvestada „täidan või selgitan“ põhimõtet, mille kohaselt finantssektori ettevõtja peab vajadusel suutma põhjendada, miks ta mõnda juhendi punkti ei rakenda või teeb seda osaliselt. Nimetatud põhimõte ei vabasta finantssektori ettevõtjat testi suhtes kohaldatavate õigusaktidest ega TIBER-EU raamistikust tulenevate kohustuslike nõuete täitmisest. Juhendis sätestatust kõrvalekaldumine võib mõjutada Finantsinspektsiooni tõendi väljastamist, kui kõrvalekalde tõttu ei ole test läbi viidud kooskõlas testi suhtes kohaldatavate nõuetega.

1.3.3. TIBER-EE testi läbiviiv finantssektori ettevõtja vastutab käesolevas juhendis kirjeldatud ülesannete täitmise eest, sealhulgas testi õiguslike ja tehniliste riskide hindamise, asjakohaste kaitsemeetmete rakendamise ning kohaldatavate õigusnormide järgimise eest.

1.3.4. Finantsinspektsioon ja EKP ei vastuta juhendi kasutamisest või TIBER-EE testi läbiviimisest tuleneva kahju eest.

### 1.4. Kontakt

1.4.1. TIBER-EE ja juhendi kohta käivate päringutega saab pöörduda Finantsinspektsiooni poole aadressil TLPT@fi.ee.

1.4.2. Käimasoleva testi kohta käivate päringutega tuleb pöörduda konkreetsele testile määratud testijuhi või tema asendaja poole.

1.4.3. Iga TIBER-EE testi läbiviiv või ettevalmistav finantssektori ettevõtja peab määrama Finantsinspektsiooni ohuteabel põhineva läbistustestimise kübertiimiga (TCT-EE) suhtlemiseks, salastatuse tagamiseks ja koordineerimiseks sobiva kontaktisiku. Määratud kontaktisikul peavad olema piisavad volitused ning asjakohane arusaam finantssektori ettevõtja kriitilistest funktsioonidest, süsteemidest ja sisemistest otsustuskorraldustest.

## 2. Juhtimiskorraldus Eestis

### 2.1. Ametlik vastuvõtmise kinnitus

2.1.1. TIBER-EU raamistiku kasutuselevõtt Eesti finantssektoris kehtestati Finantsinspektsiooni juhatuse 5. mai 2025 otsusega nr 1.1-7/67.

### 2.2. Määratud asutus

2.2.1. DORA artikli 26 lõike 9 kohaselt võib iga liikmesriik määrata finantssektoris TLPT eest vastutavaks ühe pädeva asutuse. TIBER-EU raamistikus kasutatakse selle funktsiooni kohta mõistet TIBER asutus, TLPT RTS kasutab aga mõistet ohuteabel põhineva läbistustestimise asutus. Käesoleva juhendi tähenduses käsitatakse neid mõisteid samaväärsetena.

2.2.2. Finantsinspektsioon on Eesti Vabariigi nimel tegutsev sõltumatu finantsjärelevalve- ja kriisilahendusasutus. FIS volitab Finantsinspektsiooni täitma DORA-st tulenevaid ülesandeid ning tegema küberturvalisuse alast koostööd riiklike ja Euroopa Liidu asutustega. See loob ka aluse koostööks Riigi Infosüsteemi Ametiga (edaspidi RIA) digitaalse tegevuskerksuse ja TLPT-ga seotud küsimustes.

2.2.3. TIBER-EE kohaldamisel Eestis tegutseb Finantsinspektsioon ohuteabel põhineva läbistustestimise asutusena tema TLPT pädevusse kuuluvate Eesti finantssektori ettevõtjate suhtes. EKP otsese järelevalve all olevate oluliste krediidiasutuste (Significant Institutions, edaspidi *SI-d*) kohustuslike TLPT-de puhul tegutseb ohuteabel põhineva läbistustestimise asutusena EKP.

## 2.3. Määratud asutuse roll

2.3.1. Ohuteabel põhineva läbistustestimise asutusena teeb Finantsinspektsioon järelevalvet TIBER-EE riikliku rakendamise üle. Eelkõige:

- loob ja haldab TCT-EE-d;
- koordineerib TIBER-EE testide algatamist, planeerimist ja järelevalvet;
- vaatab läbi ja valideerib peamised testidokumendid ja väljundid; ning
- väljastab testi nõuetekohase lõpuleviimise korral tõendi.

2.3.2. Finantsinspektsiooni osalus on suunatud TIBER-EE alusel läbiviidava testimise järjepidevuse, turvalisuse ja kvaliteedi toetamisele ning kooskõla tagamisele DORA, TLPT RTS-i ja TIBER-EU raamistikuga.

2.3.3. TLPT läbiviimisel piirdub Finantsinspektsiooni roll järelevalve ja kvaliteedi tagamisega. Finantsinspektsioon ei osale testi operatiivses läbiviimises. Testi läbiviimise eest vastutab testitav finantssektori ettevõtja koos tema määratud teenuseosutajatega.

2.3.4. Kui Finantsinspektsiooni TLPT pädevusse kuuluv test on läbi viidud kooskõlas kohaldatavate DORA, TLPT RTS-i, TIBER-EU ja TIBER-EE nõuetega, väljastab Finantsinspektsioon tõendi, mis kinnitab, et test viidi läbi asjakohase raamistiku ja riiklike juhtimiskorralduste alusel.

2.3.5. Kohaldatavatest nõuetest ja testi laadist tulenevalt teeb Finantsinspektsioon koostööd EKP, teiste ohuteabel põhineva läbistustestimise asutuste ja muude asjakohaste asutustega. Piiriüleste, ühiste või koondtestide koordineerimine toimub muu hulgas TLPT RTS-is sätestatud korras.

2.3.6. Finantsinspektsioon võib käesolevat juhendit vastavalt vajadusele ajakohastada, et see kajastaks TIBER-EU, DORA, RTS-i, järelevalvepraktika või riiklike rakendusvajaduste arengut.

# 3. Ohuteabel põhineva läbistustestimise kübertiim (TCT-EE)

3.1.1. Finantsinspektsioonis on TIBER-EE ja DORA kohaste TLPT-de läbiviimiseks loodud eraldi ohuteabel põhineva läbistustestimise kübertiim – TCT-EE. Lühend TCT-EE tähistab TIBER-EU raamistiku kohaselt TIBER Cyber Team mõistet ning TLPT RTS-i kohaselt TLPT Cyber Team mõistet. Käesoleva juhendi tähenduses käsitatakse neid mõisteid samaväärsetena.

3.1.2. TCT-EE tegutseb Finantsinspektsiooni finantssektori infotehnoloogiajärelevalve osakonnas ning vastutab TIBER-EE programmi igapäevase juhtimise ja rakendamise eest.

3.1.3. TCT-EE täidab koordineerivaid ülesandeid, mis on vajalikud selleks, et tagada TLPT läbiviimine kooskõlas DORA, TLPT regulatiivsete tehniliste standardite, TIBER-EU raamistiku ja käesoleva juhendiga.

3.1.4. TCT-EE koosneb testijuhtidest ja asendustestijuhtidest, kelle rollid ja vastutusalad määratakse iga testi puhul eraldi.

3.1.5. Vajaduse korral võib Finantsinspektsioon kasutada välist ekspertiisi, sealhulgas RIA ekspertiisi, järgides asjakohaseid konfidentsiaalsuse, sõltumatuse ja huvide konflikti vältimise meetmeid.

# 4. Riiklikud erisused

## 4.1. Üldine ohumaastik

4.1.1. Finantsinspektsioon võib Eesti finantssektori jaoks kättesaadavaks teha üldise ohumaastiku (Generic Threat Landscape, edaspidi GTL) dokumendi.

4.1.2. GTL annab üldise ülevaate asjakohastest küberohtudest, ohusubjektidest, taktikatest, tehnikatest ja protseduuridest ning muudest küberohukeskkonna arengutest, mis võivad olla TIBER-EE testide jaoks asjakohased.

4.1.3. GTL on toetav sisend TIBER-EE testide ettevalmistamisel. GTL-i kasutamine ei asenda testipõhise ohuteabe nõuet, mis jääb TIBER-EU raamistiku kohaselt iga TIBER-EE testi lahutamatuks osaks.

## 4.2. Konfidentsiaalsus ja infoturve

4.2.1. Kogu TIBER-EE testide raames vahetatavat teavet tuleks käsitleda testi jaoks kokku lepitud asjakohase teabe klassifitseerimise skeemi kohaselt, näiteks fooriprotokolli (Traffic Light Protocol, TLP) alusel või muu samaväärset teabekaitse taset tagava lahenduse kohaselt.

4.2.2. Kogu testi vältel tuleb kasutada turvalisi sidekanaleid. Konkreetsed suhtluskorraldused, sealhulgas krüpteerimine ja ligipääsukontrollid, tuleks kokku leppida testi ettevalmistavas etapis.

4.2.3. Kõik TIBER-EE tegevused tuleb viia läbi kooskõlas kohaldatava õigusega, sealhulgas andmekaitset, konfidentsiaalsust ja karistusõigust käsitlevate nõuetega. Eetika- ja ohutusnõudeid tuleb järgida kooskõlas TIBER-EU raamistikuga.

4.2.4. Kõiki testiandmeid, aruandeid ja nendega seotud dokumentatsiooni tuleks käsitleda piiratud juurdepääsuga teabena ning jagada rangelt vajaduspõhisel põhimõttel, et säilitada testi terviklikkus, salastatus ja turvaline läbiviimine.

4.2.5. Testitav finantssektori ettevõtja peab tagama, et väliste teenuseosutajate suhtes kehtivad samuti asjakohased konfidentsiaalsuse, sõltumatuse ja huvide konflikti vältimise nõuded.

## 4.3. Teabe ja tulemuste jagamine

4.3.1. TIBER-EE testiga seotud teabe jagamine toimub vastavalt kohaldatavale õigusele, järelevalvealasele konfidentsiaalsuskohustusele ja asjakohastele riiklikele või rahvusvahelistele koostöökokkulepetele.

4.3.2. Testidega seotud teavet ei jagata teiste riiklike või välisriikide asutustega, sealhulgas teiste järelevalvajatega, välja arvatud juhul, kui selleks on õiguslik alus

või kui testitav finantssektori ettevõtja on andnud selleks oma kirjaliku nõusoleku.

4.3.3. Kohaldatava õiguse ja koostöökokkulepete alusel võib teatavaid kõrgetasemelisi testi artefakte jagada teiste TCT-dega testimise tunnustamise, koordineerimise või järjepidevuse tagamise eesmärgil.

4.3.4. Ilma et see piiraks kohaldatavaid konfidentsiaalsusnõudeid, võib Finantsinspektsioon soodustada piisavalt üldistatud ja anonümiseeritud õppetundide jagamist, kui materjalidest on eemaldatud teave, mis võimaldab testitavat finantssektori ettevõtjat otseselt või kaudselt tuvastada, ning jagamine toetab finantssektori laiemat tegevuskerksust ega sea ohtu testitava finantssektori ettevõtja konfidentsiaalsust või turvalisust.

## 4.4. Koostöö Riigi Infosüsteemi Ametiga

4.4.1. Vajaduse korral teeb Finantsinspektsioon koostööd RIA-ga TIBER-EE, TLPT ja digitaalse tegevuskerksusega seotud küsimustes, sealhulgas ohuteabe ja tehnilise ekspertiisi kaasamiseks.

4.4.2. Koostöö RIA-ga põhineb FIS § $47^{11}$ lõike 1 punktil 4.

4.4.3. Koostöö võib vastavalt vajadusele hõlmata asjakohase teabe vahetamist, tehnilise või sisulise ekspertiisi kasutamist ning koostööd GTL-i koostamisega seotud küsimustes.

4.4.4. Igasugune koostöö peab toimuma kooskõlas kohaldatava õigusliku aluse, konfidentsiaalsusnõuete ja testi konkreetsete asjaoludega.

4.4.5. Koostöö RIA-ga ei muuda punktis 2.2. sätestatud TLPT asutuste pädevusjaotust.

## 4.5. Euroopa Keskpanga järelevalve all olevad olulised krediidiasutused

4.5.1. EKP otsese järelevalve all olevate SI-de kohustuslike TLPT-de puhul tegutseb ohuteabel põhineva läbistustestimise asutusena EKP kooskõlas kohaldatava liidu raamistikuga.

4.5.2. EKP poolt DORA alusel TLPT kohustuslasena tuvastatud SI-de kohustuslike TLPT-de suhtes kohaldatakse EKP TIBER-EU SSM rakendusjuhendit[3].

4.5.3. Kui EKP määrab TCT-EE SI TLPT järelevalvet teostavaks TCT-ks, täidab TCT-EE talle määratud ülesandeid EKP TIBER-EU SSM rakendusjuhendi kohaselt.

4.5.4. SI-de testide tõendid väljastab alati EKP.

# 5. Rakendamine

Juhend käesolevas redaktsioonis jõustub alates 15.09.2026.

[3] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guide202511.en.pdf

## Lisa 1. Lühendid

| Lühend | Tähendus | Ingliskeelne nimetus |
|---|---|---|
| DORA | Määrus, mis käsitleb finantssektori digitaalset tegevuskerksust | Digital Operational Resilience Act |
| EKP | Euroopa Keskpank | European Central Bank |
| FIS | Finantsinspektsiooni seadus | Financial Supervision Authority Act |
| GTL | Üldine ohumaastik | Generic Threat Landscape |
| RIA | Riigi Infosüsteemi Amet | Information System Authority |
| RTS | Regulatiivsed tehnilised standardid | Regulatory Technical Standards |
| SI | Oluline krediidiasutus | Significant Institution |
| TCT-EE | Eesti ohuteabel põhineva läbistustestimise kübertiim | Estonian TLPT Cyber Team |
| TIBER-EE | TIBER-EU riiklik rakendus Eestis | Estonian national implementation of TIBER-EU |
| TIBER-EU | Ohuteabel põhineva eetilise punase meeskonna testimise Euroopa raamistik | European framework for Threat Intelligence-Based Ethical Red Teaming |
| TLPT | Ohuteabel põhinev läbistustestimine | Threat-Led Penetration Testing |
| TLP | Fooriprotokoll | Traffic Light Protocol |