JUSTIITS- JA DIGIMINISTEERIUM

MINISTRI MÄÄRUS

25.08.2026 nr 30

Eesti infoturbestandard

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 ning Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" § 3 lõike 1 alusel.

1. peatükk
Üldsätted

§ 1. Määruse reguleerimisala ja eesmärk

(1) Eesti infoturbestandardi rakendamine seisneb võrgu- ja infosüsteemi infoturbe halduses ja infoturbe halduse meetmete auditeerimises.

(2) Teenuseosutajate (edaspidi *organisatsioon*) Eesti infoturbestandardi rakendamise kohustus ja ulatus on sätestatud Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" 2. peatükis.

(3) Eesti infoturbestandardi kehtestamise eesmärk on:
1) tagada avalike ning ühiskonna toimimiseks vajalike, sealhulgas oluliste ja kriitiliste ülesannete täitmiseks kasutatavate võrgu- ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase kõigis nende osades kogu elutsükli jooksul;
2) luua süsteemne raamistik, mis aitab teenuseosutajal kaitsta oma äriprotsesse, varasid, võrgu- ja infosüsteemi ning ennetada ohte ja hallata riske.

(4) Äriprotsess on organisatsiooni põhitegevuste või eesmärkide saavutamiseks vajalike tegevuste kogum, mille käigus kasutatakse aega, raha, töövahendeid ja tööjõudu (edaspidi koos *ressursid*) teenuse, toote või muu väärtust loova tulemuse pakkumiseks.

2. peatükk
Infoturbe haldus

§ 2. Infoturbe halduse süsteem

(1) Infoturbe halduse süsteemi raames vaadatakse organisatsiooni:
1) tegevusvaldkonda, eesmärke, protsesse, protseduure ja tavasid;
2) õigusaktidest ning lepingutest tulenevaid õigusi ja kohustusi;
3) keskkonda, ressursse ja vara.

(2) Infoturbe halduse toimimiseks tuleb korraldada vähemalt järgmisi tegevusi:

1) vara kasutusele võtmine – vara kogu elutsükli ulatuses infoturbe riskide tuvastamine ja hindamine, turvameetmete planeerimine ja rakendamine, sealhulgas meetmete planeerimine uue vara ja teenuste hankimise etapis või selle kavandamise käigus;
2) vara kasutamine – kasutusse antud vara kasutamise korra järgimine, infoturbekoolituste regulaarne läbimine, intsidentidele kokkuleppekohane reageerimine, sealhulgas küberintsidentidest teavitamine;
3) vara haldamine – kaitsetarbe määramise korraldamine ja kaitsetarbe saavutamiseks vajalike meetmete rakendamise regulaarne seire;
4) andmekaitse – organisatsiooni andmete või organisatsioonile usaldatud andmete kaitse korraldamine.

(3) Taasesitatavas vormis säilitatakse vähemalt järgmist teavet:
1) infoturbe halduse süsteemi alusdokumendid ja otsuste kulg;
2) infoturbesündmused ja organisatsiooni reaktsioon neile;
3) infoturbe meetmete rakendusplaan ja selles sisalduvad riskikäsitlus viisid.

§ 3. Organisatsiooni juhatuse tegevus

(1) Infoturbe halduse süsteemi toimimist korraldab organisatsiooni juhatus.

(2) Infoturbe halduse süsteemi toimimiseks juhatus:
1) määrab organisatsiooni siseselt § 2 lõikes 2 sätestatud tegevuste eest vastutajad või jätab vastutuse juhatusele;
2) eraldab vajalikud ressursid;
3) määrab kindlaks infoturbe eesmärgid, kehtestades infoturvapoliitika;
4) otsustab infoturvameetmete rakendamise plaanis kavandatud meetmete rakendamata jätmisest tulenevate riskide aktsepteerimise üle, arvestades võimalikku mõju äriprotsessile.

(3) Infoturbe halduse süsteemi korraldus peab võimaldama juhatusel saada regulaarseid ja operatiivseid ülevaateid:
1) riskidest ning nende võimalikust mõjust ja kulust;
2) toimunud küberintsidentide mõjust äriprotsessidele;
3) õigusaktides ja lepingutes sätestatud nõuetest ja nende muudatustest;
4) infoturbe hetkeseisust ja infoturvameetmete rakendamise plaani täitmisest.

§ 4. Infoturvapoliitika

(1) Infoturvapoliitikas esitatakse vähemalt:
1) turbe üldised eesmärgid ja põhimõtted, sealhulgas riskihalduse alused;
2) rollide ja vastutusalade jaotus;
3) küberintsidentide käsitlemise ja infoturbe halduse süsteemi hindamise alused;
4) viited seotud dokumentidele, sealhulgas näiteks alampoliitikad, korrad, tegevuse dokumentatsioon.

(2) Infoturvapoliitika vaadatakse üle ja vajaduse korral muudetakse vähemalt kord kalendriaastas.

§ 5. Riskihaldusmetoodika

(1) Enne riskihaldusmetoodika kasutuselevõtmist peab organisatsioon tuvastama kaitseala äriprotsessile olulised varad.

(2) Organisatsioon peab kehtestama riskihaldusmetoodika, mis on seotud organisatsiooni üldise riskihaldusega ja koosneb vähemalt järgmisest:
1) äriprotsessidele mõju avaldavate riskide tuvastamine ja hindamine, arvestades konfidentsiaalsust, autentsust, terviklust ja käideldavust;
2) vara ja äriprotsessi vastendamine infoturbekataloogi moodulitega;
3) infoturvameetmete rakendamise plaani täitmise otsused, sealhulgas riskide hindamine.

§ 6. Infoturbekataloog

(1) Infoturbekataloog (lisa 1) on organisatsiooni kahjustada võivate ohtude kaitseks võetavate meetmete loend.

(2) Lõikes 1 nimetatud meetmed jaotatakse protsessi- ja süsteemimoodulitesse.

§ 7. Infoturvameetmete rakendamise plaan

(1) Infoturvameetmete rakendamise plaan on organisatsioonikeskne struktureeritud ühest või mitmest dokumendist koosnev juhend turvameetmete haldamiseks.

(2) Infoturvameetmete rakendamise plaanis esitatakse asjakohased infoturbekataloogiga seotud meetmed. Riskihalduse põhjal lisatakse kõnealusesse rakendusplaani vajaduse korral lisameetmeid, mis on tarvilikud kaitsetarbe saavutamiseks.

(3) Infoturbekataloogi süsteemimoodulite meetmeid rakendatakse kõigile kaitseala varadele kooskõlas infoturbemeetmete rakendamise plaaniga.

(4) Infoturbekataloogi protsessimoodulite meetmed lõimitakse igapäevasesse töökorraldusse.

(5) Infoturbekataloogi meetmete rakendamise prioriteetide ja tähtaegade määramisel lähtutakse kaitsetarbest, varade omavahelisest sõltuvusest ja vara elutsükli etapist.

(6) Infoturvameetmete rakendamise plaanis võib ette näha infoturbekataloogi mooduli meetme asendamise muu samaväärse meetmega või meetme rakendamata jätmise, kui:
1) kaitsetarve on täidetud;
2) organisatsioon on riski aktsepteerinud.

(7) Meetme rakendamise tähtaeg ja tegevuste regulaarsus peab tagama kaitsetarbe saavutamise mõistliku aja jooksul. Kui meetme rakendamise tähtaeg ületab ühte aastat, tuleb seda käsitleda riskihalduses kui aktsepteeritud riski.

(8) Kui äriprotsess sõltub organisatsioonivälisest tarneahelast, hinnatakse sellega kaasnevaid riske.

(9) Organisatsioonivälise tarneahela kaitse vajaduse hindamiseks on organisatsioonil õigus nõuda väliselt osapoolelt kaitsetarvet tagavate turvameetmete rakendamist, sealhulgas seirearuandeid, asjakohase käsitlusalaga auditi järeldusotsuseid, turvasertifikaate, enesehindamise tulemusi või muud asjakohast teavet.

(10) Kui riski ei saa infoturvalisuse tagamise tõttu aktsepteerida, tuleb kaaluda alternatiivseid meetmeid või välise osapoole vahetust.

§ 8. Personali koolitamine

Organisatsioon korraldab personalile järjepidevalt koolitusi eesmärgiga:
1) parandada ja tõsta turvateadlikkust;
2) tagada teabe turvalise töötlemise ja töövahendite turvalise käitlemise oskused;
3) ennetada riskikäitumist;
4) suurendada teadlikkust küberintsidentide ennetamisest, tuvastamisest ja neile reageerimisest ning täiendada sellealaseid oskusi.

3. peatükk
Seire

§ 9. Organisatsioonisisene hindamine

(1) Organisatsioon hindab regulaarselt, kas tal on:
1) kindlaks määratud äriprotsessid;
2) kaardistatud äriprotsessidega seotud varad;
3) kindlaks tehtud välised infoturvanõuded, sealhulgas õigusaktid ja lepingud;
4) tuvastatud ja hinnatud äriprotsessidele mõju avaldavad riskid;
5) vastendatud infoturbekataloogi moodulid kaitseala varaga;
6) kehtestatud riskihaldusmetoodika;
7) koostatud infoturvameetmete rakendamise plaan;
8) rakendatud ja seiratud infoturvameetmeid vastavalt infoturvameetmete rakendamise plaanis seatud tähtaegadele;
9) kõrvaldatud auditite ja hindamiste käigus tuvastatud puudused.

(2) Lõikes 1 nimetatud hindamist võib teha organisatsiooniväline isik.

(3) Lõikes 1 nimetatud hindamise käigus tuvastatud puudused tuleb kõrvaldada ja infoturvameetmete rakendamata jätmisest tulenevad riskid aktsepteerida auditeerimise alguseks.

§ 10. Auditeerimine

(1) Auditeerimise eesmärk on hinnata, kas auditeeritava organisatsiooni infoturbe halduse süsteem ja selle raames rakendatud meetmed vastavad 2. peatüki nõuetele ning kaitsevad organisatsiooni äriprotsesse ja eesmärkide täitmist.

(2) Organisatsioonivälise audiitori sõltumatu hinnang annab organisatsioonile, selle klientidele ja partneritele teavet auditeeritava infoturbe halduse süsteemi jätkusuutlikkuse ja infoturvalisuse ohtudele vastupanuvõime kohta.

(3) Organisatsioonipoolset auditi tellimist, auditiga kaasnevaid kohustusi, auditi kvaliteedi hindamist ning audiitoripoolset auditi kavandamist, tegemist ja selle kohta aruande koostamist on kirjeldatud auditeerimiseeskirjas (lisa 2).

4. peatükk
Eesti infoturbestandardi tugi ja rakendamine

§ 11. Eesti infoturbestandardi rakendamise tugitegevused

(1) Eesti infoturbestandardi rakendamise toetamiseks ja ühtlustamiseks loob Riigi Infosüsteemi Amet asjaomase veebilehe või rakenduse.

(2) Riigi Infosüsteemi Amet võib lõikes 1 sätestatud veebilehel või rakenduses anda Eesti infoturbestandardi rakendamist toetavaid soovituslikke juhiseid ning esitada muud rakendamist toetavat ajakohast teavet.

§ 12. Enne määruse jõustumist rakendatud turvameetmete ja koostatud dokumentatsiooni kehtivus

(1) Enne käesoleva määruse jõustumist Eesti infoturbestandardi järgimiseks rakendatud turvameetmed, mis ei ole vastuolus määrusega, kehtivad kuni nende rakendamise lõppemiseni või ajakohastamiseni.

(2) Enne käesoleva määruse jõustumist Eesti infoturbestandardi järgimiseks koostatud dokumentatsioon kehtib kuni kolm aastat määruse jõustumisest.

(3) Lõikes 2 sätestatud dokumentatsiooni uuendamisel määruses sätestatud korras enne lõikes 2 sätestatud tähtaja möödumist kehtib dokumentatsioon ettenähtud korra kohaselt.

§ 13. Määruse kehtetuks tunnistamine

Ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022. a määrus nr 101 „Eesti infoturbestandard“ tunnistatakse kehtetuks.

§ 14. Määruse jõustumine

Määrus jõustub 1. septembril 2026. a.

(allkirjastatud digitaalselt)
Liisa-Ly Pakosta
justiits- ja digiminister

(allkirjastatud digitaalselt)
Tiina Uudeberg
kantsler

Justiits- ja digiministri
25.08.2026 määruse nr 30
„Eesti infoturbestandard“
lisa 1

Infoturbekataloog

Tabel 1. Protsessimoodulid

Protsessimoodulid	
GRC. Turbehaldus	
GRC.1. Infoturbe haldus üldiselt	Esitada infoturbe halduse süsteemi rajamise ja täiustamise meetmed ning turbekontseptsiooni väljatöötamise juhised
GRC.2. Infoturbe korraldus	Esitada meetmed infoturbe korralduse sobitamiseks organisatsiooniga ning infoturbe haldamiseks. Käsitletakse infoturbeprotsesside haldust ja infoturbeülesandeid organisatsioonis
GRC.3. Varade haldus	Esitada meetmed, mis tagavad organisatsiooni varade kaitse ja halduse kogu vara elutsükli vältel ning toetavad varade tervikluse säilitamist ja asutuse turvalist toimimist
GRC.4. Isikuandmete kaitse	Esitada meetmed füüsilise isiku kui andmesubjekti põhiõiguste kaitseks isikuandmete töötlemisel
GRC.5. Krüptograafia	Esitada krüptograafilise vahendi kasutamise korralduslikud meetmed ning krüptokontseptsiooni koostamise juhised
GRC.6. Vastavuse haldus	Esitada organisatsiooni eesmärkidel, õigusaktidel, lepingutel ja poliitikatel põhinevate turvanõuete kehtestamise ja järgimise meetmed
GRC.7. Audit ja läbivaatus	Esitada infoturbe auditi ja sõltumatu läbivaatuse tegemise üldised juhised, et täiustada organisatsiooni infoturvet, vältida soovimatuid suundumusi valdkonnas ja optimeerida turvameetmeid ja -protsesse
ORP. Organisatsioon ja personal	
ORP.1. Identiteedi- ja õiguste haldus	
ORP.1.1. Identiteedi- ja õiguste haldus üldiselt	Esitada identiteedi- ja õiguste halduse korraldamise meetmed. Nii kasutajad kui infotehnoloogia (edaspidi *IT*) komponendid peavad saama juurdepääsu üksnes vajalikele IT-ressurssidele ja teabele
ORP.1.2. Sotsiaalmeediakonto haldus	Esitada meetmed, mis tagavad, et organisatsiooni ametlike sotsiaalmeediakontode loomine, haldamine ja kasutamine toimub turvaliselt ühtse korra alusel
ORP.2. Personali haldus	Esitada meetmed, mille abil personaliosakond ja juht tagavad, et nii oma kui ka välised töötajad tegutsevad organisatsiooni turvaeesmärke silmas pidades
ORP.3. Töötaja infoturvateadlikkuse tõstmine	Esitada töötaja turvateadlikkuse tõstmise ja töötaja koolitusplaani koostamise meetmed, arvestades organisatsiooni spetsiifikat ja töötaja vajalikke teadmisi ja oskusi
ORP.4. Välislähetuse infoturve	Esitada meetmed andmete turvalisuse tagamiseks töötaja välislähetuses viibimisel ning abistada vastutavaid isikuid välislähetuste turvameetmete kehtestamisel

ORP.5. Teabevahetus	Esitada organisatsiooni ja välise poole vahelise turvalise teabevahetuse meetmed
ORP.6. Kaugtöö	Esitada kaugtöö raames talletatava, töödeldava ja edastatava teabe kaitse meetmed
ORP.7. IT-vahendi turvaline kasutamine	
ORP.7.1. IT-vahendi kasutamine üldiselt	Esitada meetmed, et tagada organisatsiooni töövahendi turvaline kasutamine, mis on kooskõlas infoturvanõuetega
ORP.7.2. Isikliku seadme kasutamine	Esitada meetmed, et tagada organisatsioonis isikliku töövahendi (nt isiklik mobiiltelefon, tahvelarvuti, sülearvuti, nutikell, isiklikud kõrvaklapid) turvaline kasutamine, mis on kooskõlas infoturvanõuetega
ORP.7.3. Mobiiltelefoni kasutamine	Esitada meetmed mobiiltelefoni turvaliseks kasutamiseks
ORP.8. Raadioside turvaline kasutamine	
ORP.8.1. Raadioside kasutamine üldiselt	Esitada meetmed, et tagada organisatsioonis kasutatava raadiosidetehnoloogia (nt WiFi, Bluetooth, NFC, RFID ja muud lühimaa raadioside protokollid) turvaline kasutamine, vältides volitamata juurdepääsu, andmeside pealtkuulamist ja seadmete manipuleerimist
ORP.8.2. WiFi kasutamine	Esitada organisatsiooni WiFi-võrgu kavandamise ja turvalise käitamise meetmed, et vältida volitamata juurdepääsu sidevõrgule ja andmeleket
ORP.8.3. Lähiväljaside kasutamine	Esitada meetmed, et tagada organisatsioonis lähiväljaside tehnoloogia turvaline kasutamine, mis on kooskõlas organisatsiooni infoturvanõuetega
ORP.8.4. Bluetoothi kasutamine	Esitada meetmed, et tagada Bluetoothi tehnoloogia turvaline kasutamine organisatsioonis, vältides volitamata sidumisi, andmeleket, seadmete ülevõtmist ning muid lähiväljasidega seotud riske
OPS. IT haldus	
OPS.1. IT valdkonna põhitööd	
OPS.1.1. IT haldus üldiselt	Kehtestada infoturvameetmed lahutamatu osana kõigist IT halduse põhiaspektidest (IT-varade haldamine, IT-hanked, IT käitamine, muudatuste haldus, seire, intsidentide haldus ja IT-vahendite kasutusest kõrvaldamine)
OPS.1.2. Muudatusehaldus	Esitada organisatsiooni tarkvarauuendite ja IT-süsteemide muudatusehalduse protseduuri kohaldamise, juhtimise ja optimeerimise meetmed
OPS.1.3. Andmevarundus	Esitada organisatsioonis töödeldavate andmete varunduse korraldamise meetmed
OPS.1.4. Andmete digitaalne arhiveerimine	Esitada digitaalsete dokumentide muutumatul kujul pikaajalise, turvalise ja ennistatavalt säilitamise meetmed
OPS.1.5. Turvasündmus logimine	Esitada logiandmete turvalise kogumise, talletamise ja nõuetekohase analüüsimise ja kõrvaldamise meetmed
OPS.1.6. Tarkvara testimine ja kasutuselevõtt	Esitada mistahes tarkvararakenduse või -süsteemi testimise ja kasutuselevõtu meetmed
OPS.1.7. Arvutikellade sünkroniseerimine	Esitada meetmed täpse ajaarvestuse tagamiseks IT-komponentide töös

OPS.1.8. IT-süsteemi kaughooldus	Esitada IT-süsteemi turvalise kaughoolduse korraldamise meetmed
OPS.1.9. Kaitse kahjurprogrammide eest	Esitada kahjurprogrammi vastase kaitse korraldamise meetmed
OPS.1.10. Turvanõrkuste haldus	Esitada infotehnoloogiliste turvanõrkuste haldamise protseduuride väljatöötamise meetmed koos juhistega, et minimeerida küberrünnete mõju
OPS.1.11. Andmete turvaline kustutamine	Esitada andmete turvalise kustutamise ja andmekandja hävitamise meetmed
OPS.2. IT haldus teenusena	
OPS.2.1. Väljasttellimine üldiselt	Esitada meetmed väljasttellitava teenuse turvaeesmärkide saavutamise tagamiseks kogu allhanke kestel
OPS.2.2. Pilvteenuse integratsioon äriprotsessiga	Esitada meetmed pilvteenuse kavandamiseks ja turvaliseks käitamiseks organisatsiooni äriprotsessi toetamise eesmärgil
OPS.2.3. Teenuseleping välise teenuseosutajaga	Esitada meetmed mistahes sisseostetava teenuse kvaliteedi tagamise lepete sätestamiseks teenuse osutamise lepingus (inglise keeles *service level agreement,* lühend SLA)
OPS.2.4. Tarneahela infoturve	Esitada infoturbe haldamise meetmed tarneahela nõutava turvataseme hoidmiseks, lähtudes tarneahela osalistelt nõutavatest meetmetest
OPS.2.5. X-tee andmeteenus	Esitada X-tee andmeteenuse turvalise kasutamise ja kaitse meetmed. X-tee turvaserveriga liidestatud IT-süsteem ei tohi ohustada X-tee taristut ega sattuda X-teega liidestatuse tõttu ise haavatavasse olukorda. Samuti peab andmete liikumine eri organisatsioonide ja üksuste vahel põhinema selgetel õiguslikel alustel
OPS.3. Süsteemide haldus	
OPS.3.1. Süsteemi haldus üldiselt	Esitada mistahes süsteemina käsitatava keskkonna turvalise halduse meetmed. Kuna süsteemi haldamiseks on vaja eeliskontot, tuleb rakendada meetmeid selle võimaluse väärkasutuse tõkestamiseks
OPS.3.2. Mobiilseadmete keskhaldus	Esitada mobiilseadmete halduse kavandamise ja turvalise käitamise meetmed
DER. Avastamine ja reageerimine	
DER.1. Turvaintsidendi avastamine	Esitada turvasündmusega seotud andmete kogumise, seostamise ja hindamise meetmed, et tagada turvaintsidendi terviklik ja õigeaegne avastamine
DER.2. Turvaintsidentide haldus	
DER.2.1. Turvaintsidendi käsitlus	Esitada turvaintsidendi süstemaatilise käsitlemise meetmed
DER.2.2. IT-kriminalistika võimaldamine	Esitada meetmed infoturvaintsidendi kriminalistika võimaldamiseks oluliste ettevalmistuste kaudu IT-süsteemi projekteerimise ja käigushoiu etappides
DER.2.3. Ulatusliku turvaintsidendi lahendamine	Esitada ulatusliku turvaintsidendi lahendamise meetmed

DER.3. Turvatestimine ja õppus	Esitada infoturbe nõuetelevastavuse testimise ja infoturbeõppuse korraldamise meetmed
DER.4. Talitluspidevus	Esitada meetmed infoturbe ja talitluspidevuse tagamiseks avariiolukorras

Tabel 2. Süsteemimoodulid

Süsteemimoodulid	
INF. Taristu	
INF.1. Hoone	Esitada meetmed, mis käsitlevad organisatsiooni tüüphoone tehnilisi ja korralduslikke turvaaspekte
INF.2. Hoone ruumid	
INF.2.1. Bürooruum	Esitada infoturvameetmed, mis on kohaldatavad bürooruumile (nt kontor, ladu või muu ruum, kus asub arvutitöökoht) ja bürootöökohale
INF.2.2. Serveriruum ja andmekeskus	Esitada serveriruumi ja andmekeskuse turvaliste ja jätkusuutlike käidutingimuste loomise ja säilitamise meetmed
INF.2.3. Tehnilise taristu ruum	Esitada tehnilise taristu ruumi või tehnilise taristu kapi turvalisuse tagamise meetmed
INF.2.4. Arhiiviruum	Esitada andmekandjate arhiivi ja arhiveeritaval andmekandjal oleva teabe kaitse meetmed
INF.2.5. Koosoleku-, ürituse- ja koolitusruum	Esitada koosoleku-, ürituse- ja koolitusruumis töödeldava teabe ja neis ruumides olevate IT-seadmete kaitse meetmed
INF.3. Mobiilne töökoht	Esitada mobiilsele töökohale kohaldatavad korralduslikud, tehnilised ja personali käsitlevad meetmed, mida arvestatakse ja täidetakse siis, kui töötaja töötab väljaspool organisatsiooni ruume
INF.4. Kodutöökoht	Esitada meetmed organisatsiooni teabe kaitseks ja turvalise taristu rajamiseks kodutöökohas
INF.5. Sõiduki IT-komponendid	Esitada organisatsiooni mehitatud ja mehitamata, sh isejuhtiva sõiduki infoturvameetmed juhul, kui sõiduk (nt mootor-, vee- või õhusõiduk) on varustatud tänapäevaste infotehnoloogiliste komponentidega
INF.6. Elektrikaabeldus	Esitada meetmed hoone elektritoite kaitseks rikete, häirete ja manipuleerimise eest
INF.7. Tehnosüsteemid	
INF.7.1. Hoone tehnosüsteemide haldus üldiselt	Esitada hoone või hoonete tehnoseadmete ja -süsteemide (nt kütte-, jahutus-, ventilatsiooni-, konditsioneerimis-, vee-, valgustus-, tulekaitse- ja nõrkvoolusüsteemid; inglise keeles *technical building management*, lühend TBM) kavandamise ja turvalise käitamise meetmed
INF.7.2. Hooneautomaatikasüsteem	Esitada hooneautomaatikasüsteemi (inglise keeles *building automation and control system,* lühend BACS) kavandamise ja turvalise käitamise meetmed
INF.7.3. Puhvertoiteallikas	Esitada puhvertoiteallika kavandamise ja turvalise käitamise meetmed
NET. Andme- ja kõneside	
NET.1. Arvutivõrk	
NET.1.1. Võrguhaldus üldiselt	Esitada turvalise võrguhalduse rajamise ja käigus hoidmise ning turvalise andmeside tagamise meetmed
NET.1.2. Kohtvõrk	Esitada võrgu arhitektuuri ja võrgulahenduse infoturvameetmed
NET.1.3. Raadiokohtvõrk	Esitada raadiokohtvõrgu rajamise ja turvalise käitamise juhised
NET.1.4. Virtuaalne privaatvõrk	Esitada virtuaalse privaatvõrgu kavandamise ja turvalise käitamise meetmed

NET.2. Sidevõrgu kaabeldus	Esitada meetmed sidekaabelduse kaitseks rikete, häirete ja manipuleerimise eest
NET.3. Võrgukomponendid	
NET.3.1. Võrgukomponent üldiselt	Esitada arvutivõrgu mistahes komponendi turvalise käitamise meetmed
NET.3.2. Tulemüür	Esitada tulemüüri või tulemüürisüsteemi turvalise hankimise, rajamise, konfigureerimise ja käitamise meetmed
NET.3.3. Marsruuter	Esitada ruuteri turvalise käitamise meetmed
NET.3.4. Kommutaator	Esitada kommutaatori turvalise käitamise meetmed
NET.3.5. Raadiokohtvõrgu pääsupunkt	Esitada raadiokohtvõrgu komponendi turvalise käitamise meetmed
NET.4. Võrguühenduse automaatne seadistus	Esitada võrguseadme turvalise konfigureerimise ja käitamise meetmed
NET.5. Võrkupääsu reguleerimise süsteem	Esitada meetmed arvutivõrgu klientseadme võrkupääsu reguleerimise (inglise keeles *network access control*, lühend NAC) süsteemi kavandamise ja turvalise käitamise meetmed
SYS. IT-süsteemid	
SYS.1. Serverid	
SYS.1.1. Server üldiselt	Esitada serverina kasutatavas IT-komponendis töödeldavate andmete ning sellega seotud rakenduste kaitse meetmed
SYS.1.2. Microsoft Windowsi server	Esitada Microsoft Windowsi operatsioonisüsteemiga serveri turvalise käitamise ja serverisüsteemis töödeldavate andmete ning protsesside kaitsmise meetmed
SYS.1.3. Linuxi server	Esitada Linuxi ja UNIXi operatsioonisüsteeme kasutava serverisüsteemi ja selles töödeldavate andmete ning protsesside kaitse meetmed
SYS.1.4. Riistvaraline server	Esitada riistvaralise serverisüsteemi turvalise käitamise meetmed
SYS.1.5. Virtuaalserver	Esitada virtualiseeritud serverisüsteemi turvalise käitamise meetmed
SYS.1.6. Konteinerdus	Esitada konteinertehnoloogia kavandamise ja turvalise käitamise meetmed
SYS.1.7. Kubernetes	Esitada meetmed konteinerduse haldamiseks ja andmete kaitsmiseks Kubernetese keskkonnas
SYS.2. Lõppkasutaja tööjaamad	
SYS.2.1. Tööjaam üldiselt	Esitada meetmed tööjaamas töödeldavate andmete kaitseks olenemata arvuti tüübist või selles kasutatavast operatsioonisüsteemist ning suurendada teadlikkust seadme spetsiifilistest ohtudest
SYS.2.2. Microsoft Windowsi tööjaam	Esitada Microsoft Windowsi operatsioonisüsteemi kasutava tööjaama andmete kaitse meetmed
SYS.2.3. Linuxi tööjaam	Esitada Linuxi operatsioonisüsteemi kasutava tööjaama andmete kaitse meetmed
SYS.2.4. Apple macOSi tööjaam	Esitada macOSi operatsioonisüsteemi kasutavas tööjaamas talletatud andmete kaitse meetmed
SYS.2.6. Sülearvuti	Esitada meetmed sülearvuti turvaliseks kasutamiseks organisatsioonis ja suurendada teadlikkust seadme spetsiifilistest ohtudest

SYS.2.7. Irdandmekandja	Esitada irdandmekandja (inglise keeles *removable media*) turvalise kasutamise meetmed
SYS.2.8. Failijagamisteenus	Esitada serverisõnumiploki (inglise keeles *server message block*, lühend SMB) andmesideprotokolli kavandamise ja turvalise käitamise meetmed
SYS.3. Mobiilseadmed	
SYS.3.1. Mobiilseade üldiselt	Esitada meetmed tööülesannete täitmiseks kasutatava nutitelefoni ja tahvelarvuti jaoks
SYS.3.2. Google Android	Esitada Androidi operatsioonisüsteemiga mobiilseadme turvalise haldamise meetmed
SYS.3.3. Apple iOS	Esitada iOSi ja iPadOSi operatsioonisüsteemiga mobiilseadme turvalise haldamise meetmed
SYS.4. Muud võrgustatud seadmed	
SYS.4.1. Esemevõrgu seade üldiselt	Esitada esemevõrgu (inglise keeles *internet of things*, lühend IoT) seadme turvalise haldamise meetmed
SYS.4.2. Printer ja kontorikombain	Esitada võrgustatud printeri ja kontorikombaini turvalise haldamise ja kasutamise meetmed
SYS.4.3. Sardsüsteem	Esitada sardsüsteemi (inglise keeles *embedded system)* turvalise kasutamise meetmed
SYS.5. Serveriteenused	
SYS.5.1. Serveriteenus üldiselt	Esitada mistahes serveriteenuse turvalise seadistamise ja haldamise meetmed
SYS.5.2. Failiserver	Esitada failiserveri turvalise käitamise meetmed
SYS.5.3. Andmebaasiserver	Esitada andmebaasisüsteemi kavandamise ja turvalise käitamise ning andmebaasides töödeldava teabe kaitsmise meetmed
SYS.5.4. Veebirakendus	Esitada veebirakenduse turvalise töötamise ning töödeldava teabe kaitsmise meetmed
SYS.5.5. Ajaserveri teenus	Esitada meetmed ajaserveri turvaliseks seadistamiseks usaldusväärse ja täpse kellaaja tagamise eesmärgil kõigis seotud IT-süsteemides
SYS.5.6. Domeeninimesüsteem	Esitada organisatsioonis kasutatava domeeninimesüsteemi (inglise keeles *domain name system,* lühend DNS) serveriteenuste turvalise käitamise meetmed
SYS.5.7. Veebiserver	Esitada veebiserveri ja veebiserveri kaudu juurdepääsetava teabe kaitse meetmed
SYS.5.8. Andmesalvesti	Esitada andmesalvestilahenduse kavandamise, turvalise käitamise ja kasutuselt kõrvaldamise meetmed
SYS.5.9. Terminaliserver	Esitada terminaliserveri kavandamise ja turvalise käitamise meetmed
SYS.5.10. E-posti server	Esitada e-posti serveri turvalise seadistamise ja käitamise meetmed
SYS.5.11. Microsoft Exchange	Esitada Microsoft Exchange'i rühmatarkvaralahenduse kavandamise ja turvalise käitamise meetmed
SYS.5.12. Kataloogiteenus	Esitada kataloogiteenuse kavandamise, turvalise käitamise ja kõrvaldamise ning kataloogiteenuse andmete kaitsmise meetmed
SYS.5.13. Microsoft Active Directory Domain Services	Esitada meetmed Microsoft Active Directory Domain Services'i tavakasutuse turbeks, kui Active Directory teenust kasutatakse

	Microsoft Windowsi süsteemidest koosneva taristu ja keskse autentimis- ja autoriseerimislahenduse haldamiseks
SYS.5.14. X-tee turvaserver	Esitada X-tee turvaserveri kaitse meetmed, et tagada andmevahetuse tõendusväärtus ja X-teega seotud äriprotsesside usaldusväärsus
SYS.5.15. Tehisarusüsteem	Esitada meetmed tehisarusüsteemi turvaliseks kasutuselevõtmiseks ja käitamiseks organisatsioonis
SYS.5.16. IP-telefonside server	Esitada VoIP-põhise sidesüsteemi komponendi ja IP-telefoni kõneedastuse turvalisuse tagamise meetmed
SYS.5.17. Virtualiseerimissüsteem	Esitada serveri virtualiseerimiskeskkonna turvalisuse tagamise meetmed
SYS.5.18. Töölaua virtualiseerimine	Esitada virtuaaltöölaua taristu (inglise keeles *virtual desktop infrastructure*, lühend VDI) kavandamise ja turvalise käitamise meetmed
SYS.5.19. Elektrooniline arhiivisüsteem	Esitada digitaalsete andmete arhiveerimise süsteemi kavandamise ja turvalise käitamise meetmed
SYS.5.20. Keskne logitaristu	Esitada keskse logitaristu kavandamise ja käitamise meetmed
SYS.6. Pilvandmetöötlus	
SYS.6.1. Pilvandmetöötlus üldiselt	Esitada pilvandmetöötluse kavandamise ja turvalise käitamise meetmed
SYS.6.2. Pilvrakendus	Esitada pilvrakenduse turvalise seadistamise ja käitamise meetmed
SYS.7. Käidutehnoloogia	
SYS.7.1. Käidutehnoloogia üldiselt	Esitada korralduslikud ja kontseptuaalsed meetmed käidutehnoloogia (inglise keeles *operational technology*, lühend OT) turvaliseks kasutamiseks organisatsioonis
SYS.7.2. Tööstusautomaatika	Esitada tööstusautomaatikasüsteemi (inglise keeles *industrial automation and control system*), sh protsessijuhtimissüsteemi (inglise keeles *industrial control system*, lühend ICS) ja SCADA-süsteemi komponentide turbe meetmed, olenemata komponentide valmistajast, arhitektuurist, otstarbest ja paigalduskohast
SYS.7.3. Autonoomnesüsteem	Esitada autonoomse süsteemi, sh nutika anduri, andurina töötava seadmestiku ja robotseadme turbe meetmed, olenemata selle valmistajast, otstarbest, arhitektuurist või asukohast
SYS.7.4. Ohutusautomaatika	Esitada infoturvameetmed ohutusautomaatika süsteemi turvaliseks kasutuselevõtmiseks ja käitamiseks
SYS.7.5. Programmeeritav kontroller	Esitada programmeeritava kontrolleri (inglise keeles *programmable logic controller*, lühend PLC) turvalise kasutuselevõtmise ja käitamise meetmed, olenemata nende valmistajast, otstarbest, arhitektuurist või asukohast
SYS.7.6. Käidutehnoloogia komponentide kaughooldus	Esitada käidutehnoloogia komponentide turvalise kaughoolduse meetmed. Käidutehnoloogia koosneb tavaliselt eri tootjate riistvara- ja tarkvarakomponentidest, mille käigushoidmiseks ja hooldamiseks tuleb tagada volitatud hoolduspersonali kaugjuurdepääs
APP. Lõppkasutaja rakendused	

APP.1. Tarkvara üldiselt	Esitada lõppkasutaja tööjaamas kasutatava tarkvara ja tarkvaraga töödeldavate andmete turbe meetmed, sh tarkvara kasutuselevõtmise, hankimise, kasutamise ja kasutuselt kõrvaldamise meetmed
APP.2. Veebilehitseja	Esitada meetmed andmete kaitsmiseks tööjaama veebilehitseja kaudu realiseeruda võivate ohtude eest, hõlmates nii tsentraalselt kui ka iseseisvalt hallatavaid töökeskkondi
APP.3. E-posti klient	Esitada e-posti kliendi töödeldavate andmete kaitse üldmeetmed
APP.4. Kontoritarkvara	Esitada kontoritarkvaras töödeldavate andmete kaitsmise ja kontoritarkvara turvalise haldamise meetmed
APP.5. Rühmatarkvara	Esitada ühendatud side- ja koostöölahenduse (inglise keeles *unified communication and collaboration*, lühend UCC) turvalise kasutamise meetmed
APP.6. Mobiilirakendus	Esitada äriprotsessi toetavas mobiilirakenduses töödeldavate andmete kaitse meetmed
DEV. Tarkvaraarendus	
DEV.1. Tarkvaraarendus üldiselt	Esitada organisatsiooni tellitud või organisatsioonis arendatava tarkvaralahenduse infoturbe haldamise ja tarkvara turvalisuse tagamise meetmed
DEV.2. Tarkvaraarendusprojekt	Esitada organisatsiooni individuaalseks kasutusotstarbeks välja töötatud või organisatsiooni tarbeks oluliselt kohandatud rakenduste projektipõhise arendamise meetmed
DEV.3. Veebirakenduse arendus	Esitada dünaamilise (muutuva sisuga) veebirakenduse turvalise arendamise ja veebirakenduses töödeldavate andmete kaitsmise meetmed
DEV.4. Integreerimine Eesti e-riigi teenustega	
DEV.4.1. eID komponent	Esitada meetmed elektroonilise identiteedi (eID) komponendi ja sellega seotud teenuste rakendamiseks organisatsioonis

Justiits- ja digiministri
25.08.2026 määruse nr 30
„Eesti infoturbestandard“
lisa 2

Auditeerimiseeskiri

1. Terminid

Käesolevas lisas kasutatakse järgmisi termineid:
audiitor – (inglise keeles *auditor*) audiitorettevõttele auditi raames tööd tegev isik;
audiitorettevõte – (inglise keeles *auditing entity*) juriidiline isik, kes osutab võrgu- ja infosüsteemide auditeerimise teenust;
audit – auditeerimine määruse § 10 lõikes 1 sätestatud eesmärgil;
auditeeritav – (inglise keeles *auditee*) teenuseosutaja (edaspidi *organisatsioon*) või selle osa, keda või mida auditeeritakse, või auditi tellinud organisatsioon;
auditi käsitlusala – (inglise keeles *audit scope*) auditi või läbivaatuse ulatus ja piirid, millega määratakse muu hulgas kindlaks auditeeritavad või läbivaadatavad tegevuskohad, organisatsiooni üksused, protsessid, funktsioonid, süsteemid, varad ja tarneahela haldus;
auditirühm – audiitorettevõtte poolt auditi tegemiseks audiitoritest ja tehnilistest ekspertidest moodustatud rühm;
juhtivaudiitor – (inglise keeles *lead auditor*) auditirühma juhtiv audiitor;
teenuseandja – füüsiline või juriidiline isik, kes teeb digielemente sisaldava toote tarbijale vahetult või kellegi kaudu turul tasuta või tasu eest kättesaadavaks või kes annab tarbijale vahetult või kellegi kaudu tasuta või tasu eest digielemente sisaldava tootega seotud teenuse.

2. Auditi üldine korraldus

2.1. Auditi tegemiseks sõlmitakse audiitorettevõttega auditeerimisleping ja konfidentsiaalsusleping.

2.2. Auditi riski vähendamiseks ei tohi audiitorettevõte ja juhtivaudiitor teha järjest üle kahe sama organisatsiooni auditi.

2.3. Auditeeritav määrab auditi tegemise ajaks kontaktisiku või -isikud.

2.4. Auditi tegemine plaanitakse koostöös auditeeritava kontaktisikuga, kes tagab vajalike andmete ja isikute kättesaadavuse auditi ajal. Põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teha kaugtöö vormis, sellisel juhul kajastatakse see fakt auditi lõpparuandes ja auditi järeldusotsuses koos kaugtöö vormis tehtud auditi käsitlusala kirjeldusega.

3. Auditi tellimine või hankimine

3.1. Auditit tellides või hankides kirjeldab auditeeritav üheselt ja arusaadavalt auditi käsitlusala, sealhulgas auditeeritavat äriprotsessi, sellele määratud kaitsetarvet ning äriprotsessi erisusi. Käsitlusala peab hõlmama vähemalt küberturvalisuse seaduse § 3 lõigetes 2–5 nimetatud tegevusaladega seotud võrgu- ja infosüsteeme.

3.2. Auditeeritav esitab audiitorettevõttele rakendamisele määratud infoturbekataloogi moodulite nimekirja, andmetöötluse tegevuskohad, kasutatavad töökeeled, arvutikasutajate arvu, infotehnoloogia (edaspidi *IT*) meeskonna suuruse, IT-taristu lühikirjelduse ja väljasttellitavate IT-teenuste loendi.

3.3. Kui auditi käsitlusalasse kuuluvaid andmeid töödeldakse mitmes auditeeritava tegevuskohas, esitab auditeeritav lepingus minimaalse tegevuskohtade arvu, mille suhtes audit tehakse. Tegevuskohtade valik ja tegevuskohtade arv peab tagama kõikide tegevuskohatüüpide proportsionaalse esindatuse. Kui andmeid töödeldakse kolmes või vähemas tegevuskohas, välja arvatud pilvteenuse tarnija tegevuskoht, tehakse auditiprotseduurid kõigis tegevuskohtades.

3.4. Auditeeritav märgib auditit tellides või hankides ära, kui tegevuskohas ei ole võimalik kohapeal auditiprotseduure teha (nt õigusaktidest või teenuseandjaga sõlmitud kokkulepetest tulenevalt).

3.5. Auditi võib tellida või hankida mitmele auditeeritavale korraga. Kui auditeeritavad tuginevad samale infoturbe halduse süsteemile (nt on neil ühine infoturbe organisatsioon, infoturvapoliitika ja infoturbe dokumentatsioon), võib ühe auditi käsitlusala laiendada mitmele auditeeritavale. Seejuures käsitletakse auditiaruandes ja järeldusotsustes vajaduse korral auditeeritavate erisusi.

3.6. Kui auditeeritav vahetab audiitorettevõtet, lisab ta hankedokumentatsiooni kehtiva auditi järeldusotsuse.

3.7. Auditi hankedokumentatsiooni või tellimuse põhjal peab audiitorettevõttel olema võimalik adekvaatselt hinnata auditiprotseduuride tegemisega seotud tööaega ja kulu. Auditi eest küsitava tasu määramisel tugineb audiitorettevõte muu hulgas punktis 3.8 sätestatule.

3.8. Audiitorettevõte esitab auditipakkumuses audiitori töömahu prognoosi ja eeldatava ajaplaani. Soovitav on lisada ka auditeeritava töötajatele auditiga kaasneva töömahu prognoos. Auditiprotseduuridele kuluvate tundide arv moodustab vähemalt 60% auditiks kavandatud töötundide koguarvust.

4. Nõuded audiitorile

4.1. Auditeerimist juhib vastava kutseoskusega juhtivaudiitor. Juhtivaudiitor vastutab auditi käigus tehtavate tööde eest ning allkirjastab auditi lõpparuande ja järeldusotsuse.

4.2. Juhtivaudiitoril peab auditi tegemise ajal kehtima vähemalt üks järgmine kutsetunnistus:
4.2.1. ülemaailmse IT-professionaale ühendava organisatsiooni ISACA välja antud infosüsteemide audiitori (inglise keeles *Certified Information Systems Auditor,* lühend *CISA*) kutsetunnistus;
4.2.2. kvaliteediinstituudi (inglise keeles *Chartered Quality Institute*) rahvusvahelise kutsetunnistusega audiitorite registri (inglise keeles *International Register of Certificated Auditors*, lühend *IRCA*) välja antud infoturbe halduse süsteemide ISO/IEC 27001 kohase sertifitseerimisskeemi põhine juhtivaudiitori kutsetunnistus;
4.2.3. ametialase hindamise ja kutsetunnistuste andmise nõukogu PECB välja antud infoturbe halduse süsteemide ISO/IEC 27001 kohase sertifitseerimisskeemi põhine juhtivaudiitori kutsetunnistus.

4.3. Juhtivaudiitor peab auditile eelnenud kolme aasta jooksul olema audiitorina osalenud vähemalt kolmes infoturbe või IT-süsteemide halduse auditis, nt Eesti infoturbestandardi auditis. Juhtivaudiitoril peab olema vähemalt nelja-aastane IT auditi, IT juhtimise või infoturbealane töökogemus.

4.4. Auditirühma kaasatud audiitoritel peab olema vähemalt kahe-aastane IT auditi, IT juhtimise või infoturbealane töökogemus.

4.5. Auditirühma kaasatud tehnilistel ekspertidel peab olema auditi käsitlusala spetsiifikale vastav tehniline kvalifikatsioon või vähemalt kahe-aastane IT halduse või infoturbealane töökogemus.

4.6. Auditirühma liikmed peavad olema auditeeritavast sõltumatud ja ei tohi olla osalenud auditeeritava infoturbe halduse süsteemi kavandamises või rakendamises, sh auditeeritava konsulteerimises auditeeritavas valdkonnas, auditi alguskuupäevale eelnenud kolme aasta jooksul.

4.7. Auditirühma liikmete sõltumatus peab olema kinnitatud allkirjastatud deklaratsiooniga.

4.8. Auditirühma liikmed peavad tagama oma kohustuste täitmise käigus teatavaks saanud teabe hoidmise teadmisvajaduspõhiselt ning mitte jagama teavet auditeeritava nõusolekuta. Auditeeritava esitatud isikuandmete töötlemisel, sh isikuandmeid sisaldavate dokumentide läbivaatamisel ning logiandmete ja tuvastussüsteemide andmete kasutamisel, järgib audiitor muu hulgas andmekaitsealaste õigusaktide nõudeid.

4.9. Audiitor peab auditi tegemisel järgima tunnustatud auditeerimisstandardeid ja -suuniseid, infoturbe parimaid tavasid ja audiitori kutse-eetika koodeksit (nt ISACA kutse-eetika koodeks).

4.10. Audiitor peab auditi kavandamisel ja tegemisel juhinduma auditi käsitlusalast, määruse 2. peatüki nõuetest ja õigusaktidest. Auditiprotseduuride tegemisel ja meetmete valimi koostamisel arvestatakse infoturvaohtudest lähtuvaid riske ja auditeeritava kaitsetarvet ning nende alusel hinnatakse asjakohaste infoturbekataloogi meetmete rakendatust.

5. Audit

5.1. Auditi alguseks peavad organisatsioonisisese hindamise käigus tuvastatud puudused olema kõrvaldatud ja infoturvameetmete rakendamata jätmisest tulenevad riskid aktsepteeritud. Puuduste kõrvaldamata jätmise korral on audiitorettevõttel õigus nõuda auditi alguse edasi lükkamist.

5.2. Enne auditi algust koostatakse ja kooskõlastatakse auditeeritavaga auditi plaan. Auditi plaan aitab tagada, et kriitilistele infoturbevaldkondadele pööratakse auditi käigus piisavalt tähelepanu ja auditiprotseduurid tehakse õiges järjekorras. Olude muutudes või ootamatute asjaolude ilmnedes muudetakse vastavalt ka auditi plaani.

5.3. Auditi käigus hinnatakse:
- 5.3.1. organisatsiooni infoturbe halduse süsteemi vastavust määruse 2. peatüki nõuetele;
- 5.3.2. infoturbe dokumentatsiooni aja- ja asjakohasust;
- 5.3.3. infoturvameetmete rakendamise asjakohasust, riskipõhisust ning proportsionaalsust.

5.4. Infoturbe dokumentatsiooni asjakohasuse ja meetmete proportsionaalsuse hindamisel võetakse igakülgselt arvesse auditeeritava riskidele avatuse määra, organisatsiooni suurust ning intsidentide esinemise võimalikkust ja nende tõsidust, sealhulgas nende ühiskondlikku ja majanduslikku mõju.

5.5. Audiitor hindab infoturvameetmete rakendamise plaani alusel meetmete rakendatust ning moodulite väljajättude asjakohasust ja proportsionaalsust auditi käsitlusala ulatuses. Meetmete rakendamist kontrollitakse valikuliselt, vastavalt kinnitatud auditi plaanile. Kontrollitavate meetmete valimisel lähtub audiitor:
- 5.5.1. äriprotsessile mõju avaldavatest ohtudest ja riskidest;
- 5.5.2. mooduliga seotud ohtude olulisusest organisatsiooni kontekstis;
- 5.5.3. auditeeritavas organisatsioonis teostatud infoturvariskide kaalutlemise tulemustest;
- 5.5.4. organisatsioonis toimunud infoturvaintsidentidest;
- 5.5.5. varasemate infoturbe auditite leidudest ning läbivaatuste aruannetes esitatud tähelepanekutest ja soovitustest;
- 5.5.6. auditeeritavale eelnevalt tutvustatud meetmetest valimi moodustamise metoodikast.

5.6. Audiitor lähtub oma hinnangutes riskipõhisuse printsiibist. Audiitori tähelepanek võib põhineda ühe või mitme meetme mitterakendamisel või meetmete osalise rakendamise koosmõjul.

5.7. Hinnangu kujundamiseks teeb auditirühm auditiprotseduure, mille maht moodustab vähemalt 60% auditi kogumahust ja mis hõlmab vähemalt järgmisi protseduure:
- 5.7.1. intervjuud;
- 5.7.2. meetmete tõhususe kontroll, sh tehniline kontroll;
- 5.7.3. paikvaatlused;
- 5.7.4. dokumentatsiooni ja tõendusmaterjali läbivaatus.

5.8. Auditi tõendusmaterjali võib auditeeritav audiitorile kas väljastada, kohapeal näidata või selgitada intervjuu käigus (nt võrguskeem, logide analüsaator, tulemüüri reeglid, õiguste süsteemi selgitamisel reaalsed isikupõhised näited).

5.9. Kui tõendusmaterjalidega tuleb tutvuda kohapeal, tagatakse audiitorile selleks vajalik töökoht ja töötingimused.

5.10. Auditeeritava teenuseandja infoturbe hindamisel tuginetakse hinnangut kujundades teenuseandja (nt pilvteenuse tarnija) esitatud auditi käsitlusala hõlmavatele ja turvameetmete rakendatust kinnitavatele sertifikaatidele ning vastavusauditite aruannetele. Hinnangu kujundamisel võib arvesse võtta ka lepingulisi infoturvanõudeid, organisatsiooni koostatud riskihinnangut teenuseandja teenuse kohta ja riskihinnangust lähtuvate meetmete rakendamist.

5.11. Audit lõpeb auditi lõpparuande ja järeldusotsuse esitamisega auditeeritavale.

6. Auditi lõpparuanne ja auditi järeldusotsus

6.1. Lõpparuanne koosneb kahest eraldi ja juhtivaudiitori digiallkirjastatud elektroonilisest dokumendist: auditi järeldusotsusest ja auditi lõpparuandest.

6.2. Auditi järeldusotsus peab sisaldama vähemalt järgmist:
6.2.1. auditeeritava ametlik nimetus ning auditi käsitlusalasse kuuluvate organisatsioonide ametlik nimetus ja registrikood;
6.2.2. auditi tegemise aeg ja kestus;
6.2.3. käsitlusala;
6.2.4. üldhinnang organisatsiooni infoturbe halduse süsteemi toimimisele. Üldhinnang sisaldab muu hulgas teavet, kas ja kui palju leiti auditi käigus lahknevusi ja sellest tulenevaid kõrge tasemega riske;
6.2.5. audiitorettevõtte ametlik nimetus ja auditi teinud auditirühma liikmete nimed.

6.3. Auditi järeldusotsus ei või sisaldada juurdepääsupiiranguga teavet.

6.4. Auditi lõpparuanne peab sisaldama vähemalt järgmist:
6.4.1. auditi kokkuvõte, mis sisaldab juhtivaudiitori nime, auditi tegemise aega, auditi tulemuste lühikokkuvõtet ning auditirühma üldhinnangut infoturbe halduse süsteemi toimimisele. Auditi kokkuvõttes esitatakse ka auditi käigus kinnitust saanud positiivsed aspektid;
6.4.2. auditi käsitlusala, sh äriprotsesside loend ja nende peamised ohud;
6.4.3. auditi metoodika, ajaplaan, auditeeritud tegevuskohad ja auditi tegemisel esinenud piirangud;
6.4.4. auditis osalenud auditeeritava töötajate ja auditirühma liikmete nimekiri ning nende rollide kirjeldused;
6.4.5. auditirühma hinnang IT-riskide haldusele;
6.4.6. auditirühma hinnang infoturvameetmete rakendamisele;
6.4.7. auditi leiud koos lahknevuste kirjelduste ja auditirühma lisatud riskihinnangutega;
6.4.8. auditi lõpparuande lisadena vormistatud asjakohane tõendusmaterjal.

6.5. Mitmele auditeeritavale korraga ühise auditi tegemisel käsitlevad auditi järeldusotsus ja lõpparuanne vajaduse korral ka auditeeritavate erisusi. Kokkuleppel võib iga auditeeritava kohta koostada eraldi lõpparuande ja järeldusotsuse, viidates otsuses auditi ühisele käsitlusalale.

6.6. Infoturbe halduse süsteemi hindamisel peab audiitorettevõte arvestama vähemalt järgmisi aspekte:
6.6.1. süsteem vastab määruse 2. peatüki nõuetele;
6.6.2. organisatsioonis on määratud infoturbe eest vastutajad ja infoturbele on eraldatud piisavad ressursid;
6.6.3. organisatsioonis on määratud kaitseala ja äriprotsessiga seotud varad;
6.6.4. organisatsioonis on tuvastatud ja hinnatud äriprotsessi nõuetelevastavust rikkuda võivad ohud ja riskid;
6.6.5. organisatsioonis on teostatud infoturbe haldus, sh valitud meetmed vastavad riskihaldusmetoodikale, et leevendada organisatsiooni äriprotsessi toimimisele mõju avaldavate riskide kahjulikke tagajärgi.

6.7. Aruandes esitatakse iga sellise auditileiu kirjeldus, lahknevus infoturbe halduse süsteemi nõuetest, leiuga kaasneva riski kirjeldus ja auditirühma soovitus riski käsitlemiseks:
6.7.1. millest tulenevad ühele või mitmele äriprotsessile madala tasemega riskid;
6.7.2. millest tulenevad ühele või mitmele äriprotsessile kõrge tasemega riskid;
6.7.3. mille riskid üksikult võttes on madala tasemega, kuid mille puhul võib leidude koosmõju tõttu asjaolude ebasoodsal kokkusattumisel kaasneda kõrge tasemega risk ühele või mitmele äriprotsessile.

6.8. Auditirühm analüüsib meetmete mitterakendamise põhjendusi ning hindab meetmete rakendamata jätmisest või osalisest rakendamisest tulenevaid riske järgmiselt:
6.8.1. kõrge tasemega risk – oluline lahknevus meetmetes kirjeldatu ja tegeliku olukorra vahel. Meetmete rakendamata jätmisest tulenevate riskide realiseerumine võib tekitada suurt kahju

organisatsiooni varadele ja tegevusele. Kahju põhjustab lepingute ja õigusaktide täitmata jätmist ning võib ähvardada äriprotsesside jätkusuutlikkust või auditeeritava olemasolu;

6.8.2. madala tasemega risk – väheoluline lahknevus meetmetes kirjeldatu ja tegeliku olukorra vahel. Riskide realiseerumine võib tekitada piiratud ja ohjatavat kahju auditeeritava varadele ja tegevusele (nt lühiajalised töökatkestused).

6.9. Auditi lõpparuandes esitatakse loend auditi käigus:

6.9.1. tehtud auditiprotseduuridest ja kogutud tõendusmaterjalidest;

6.9.2. kontrollitud moodulistest.

6.10. Auditi leidude kohta on auditirühmal olemas tõendusmaterjal, auditi kontrollid peavad olema korratavad.

6.11. Kui auditi tegemisel tuginetakse varasema infoturbe halduse süsteemi auditi tulemustele, märgitakse auditi aruandes selgelt, millisele auditi aruandele auditirühm on tuginenud ja mil määral.

6.12. Auditi järeldusotsuse ja auditi lõpparuande kavand esitatakse auditeeritavale seitsme päeva jooksul pärast auditiprotseduuride lõppemist.

6.13. Auditeeritaval on õigus esitada 14 päeva jooksul kavandi kohta audiitorettevõttele kirjalikult taasesitatavas vormis vaidlustus, sealhulgas täiendavaid tõendusmaterjale.

6.14. Vaidlustuse arvestamise korral teeb audiitorettevõte 14 päeva jooksul kavandis asjakohased parandused. Vaidlustuse arvestamata jätmise korral lisab audiitorettevõte auditi lõpparuandele vaidlustuse ja selle arvestamata jätmise põhjenduse.

6.15. Auditi järeldusotsus ja auditi lõpparuanne esitatakse auditeeritavale hiljemalt 14 päeva jooksul pärast vastavalt punktis 6.13 või 6.14 sätestatud tähtaja möödumist. Auditeeritav kinnitab auditi lõpparuande vastuvõtmise kirjalikult taasesitatavas vormis.

6.16. Kokkuleppel auditeeritavaga võib audiitorettevõte tutvustada auditi lõpparuannet auditeeritava juhtkonnale.

6.17. Auditeeritav esitab järelevalveasutusele auditi järeldusotsuse hiljemalt 14 päeva jooksul pärast auditi järeldusotsuse ja auditi lõpparuande saamist.

6.18. Kui auditi järeldusotsuses on viidatud ühele või mitmele kõrge tasemega riskile, tuleb auditeeritaval esitada järelevalveasutusele ka auditi lõpparuanne.

6.19. Organisatsioon võib Vabariigi Valitsuse 19. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 4 lõikes 1 sätestatud auditite vahelisel perioodil esitada järelevalveasutusele uuendatud auditi järeldusotsuse.

7. Auditijärgsed tegevused

7.1. Auditeeritav kavandab parandusmeetmete rakendamise, määrab vastutajad ja tähtajad. Parandusmeetmete rakendamist ja infoturvameetmete rakendamise plaani ajakohastamist koordineerib infoturbe eest vastutav isik.

7.2. Auditeeritav kõrvaldab auditi lõpparuandes viidatud madala tasemega riski või määrab käsitlusviisi hiljemalt järgmise auditi alguseks.

7.3. Kõrge tasemega riski on auditeeritav kohustatud kõrvaldama kuue kuu jooksul auditi järeldusotsuse ja auditi lõpparuande saamisest arvates. Kui auditeeritaval ei õnnestu kuue kuu jooksul seda riski kõrvaldada, koostab ta riski käsitlemise plaani, milles kirjeldab riski vähendamiseks rakendatud meetmeid ja riski kõrvaldamiseks rakendatavaid ajutisi meetmed ning määrab plaani rakendamise eest vastutaja.

7.4. Punktis 7.3 sätestatud kohustuse täitmisest teavitab auditeeritav järelevalveasutust 14 päeva jooksul kohustuse täitmisest arvates.

7.5. Punktis 7.3 sätestatud plaani koostamisest teavitab auditeeritav järelevalveasutust 14 päeva jooksul plaani koostamisest arvates, kuid hiljemalt kuue kuu pärast auditi järeldusotsuse ja auditi lõpparuande saamisest arvates.

7.6. Kui auditi aruannete säilitamise tähtaeg ei tulene muust õigusaktist või eeskirjast, säilitab auditeeritav auditi aruandeid turvaliselt vähemalt seitse aastat.

7.7. Audiitorettevõte säilitab auditi aruandeid ja seotud dokumente turvaliselt ning vastavalt pooltevahelisele kokkuleppele. Juurdepääs dokumentidele on üksnes vastava teadmisvajadusega isikul.