

Majandus- ja infotehnoloogiaministri a määrus nr ...
„Ettevõtlus- ja infotehnoloogiaministri
16. detsembri 2022 määruse
nr 101 „Eesti infoturbestandard“ muutmine“
Lisa 3

Eesti infoturbestandard

Auditeerimisjuhend

Sisukord

1. Sissejuhatus.....	3
2. Mõisted ja lühendid.....	3
3. E-ITS auditi eesmärk.....	4
4. Auditi kohustus.....	4
5. E-ITS auditi eeldused.....	4
6. Auditi üldine korraldus.....	5
7. E-ITS auditi tellimine.....	5
8. Nõuded E-ITS audiitorile.....	6
9. E-ITS eelaudit.....	7
10. E-ITS põhiaudit.....	7
11. E-ITS vaheaudit.....	8
12. Lõpparuanne ja järeldusotsus.....	8
13. Auditijärgsed tegevused.....	10
14. Seonduvad dokumendid.....	11

1. Sissejuhatus

- 1.1. Käesolev dokument annab juhiseid Eesti infoturbestandardi (edaspidi E-ITS) põhise sõltumatu auditi (edaspidi E-ITS audit, audit) läbiviimiseks. E-ITS auditite läbiviimise üldised põhimõtted on sätestatud määruses „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (kehtestatud küberturvalisuse seaduse §7 lõike 5 alusel).
- 1.2. Juhend on mõeldud auditi läbiviijale (E-ITS audiitor, audiitorettevõtte), auditi tellijale ja auditeeritavale organisatsioonile (E-ITS rakendav organisatsioon, asutus, ettevõtte). Auditeeritav organisatsioon saab juhendi põhjal ülevaate auditi läbiviimise eeltingimustest, auditi hanke ettevalmistamisest, kohustustest auditi käigus ja auditi kvaliteedi hindamisest. E-ITS audiitorile annab juhend juhised auditi kavandamiseks, läbiviimiseks ja aruande vormistamiseks.

2. Mõisted ja lühendid

N r	Termin või lühend	Lähtekeeles (inglise/saksa)	Lühike definitsioon
1	audiitor (E-ITS audiitor)	auditor	E-ITS auditit läbi viiv isik, auditirühma liige
2	auditeeritav	auditee	Organisatsioon või selle osa, mida auditeeritakse
3	audiitorettevõtte	auditing entity	Auditeerimislepingu alusel E-ITS auditit teostav ettevõtte (vt p 6. <i>Auditi üldine korraldus</i>)
4	auditirühm	audit team	Audiitoritest ja tehnilistest ekspertidest koosnev rühm auditite läbiviimiseks
5	audititsükkel	-	Määrusest tulenev E-ITS auditeerimisperiood kolm aastat
6	E-ITS audit, audit	-	Eesti infoturbestandardi põhine sõltumatute pädevate isikute sooritatav süstemaatiline, sõltumatu ja dokumenteeritud protsess infoturbe halduse süsteemi ja infoturbe protsesside läbivaatuseks, asitõendite kogumiseks, asitõendite objektiivseks hindamiseks ja tulemuste teatamiseks auditeeritavale
7	juhtaudiitor	lead auditor	E-ITS audiitor, kes juhib auditirühma tööd, vastutab auditi läbiviimise eest ja allkirjastab auditi aruanded. Juhtaudiitoril on olemas auditi läbiviimiseks vajalik kvalifikatsioon (p 8. <i>Nõuded E-ITS audiitorile</i>)
8	käsitlusala	scope	Auditi kontekstis: Auditi käsitlusalasse kuuluvad äriprotsessid ja sihtobjektid
9	lahknevus	nonconformity	Erinevus standardi kohalduva osa ja tegeliku olukorra vahel

3. E-ITS auditi eesmärk

- 3.1. E-ITS auditi eesmärk on hinnata, kas auditeeritava organisatsiooni infoturbe halduse süsteem ning selle raames rakendatud meetmed on vastavuses dokumendiga „E-ITS Nõuded infoturbe halduse süsteemile” ning on piisavad organisatsiooni äriprotsesside kaitseks ja organisatsiooni eesmärkide täitmiseks.
- 3.2. Audiitori sõltumatu hinnang annab organisatsioonile, selle klientidele ja partneritele kindlustunde organisatsiooni jätkusuutlikkuse ja infoturbe ohtudele vastupanuvõimekuse osas.
- 3.3. E-ITS auditi läbiviimisel arvestatakse infoturbe ohtudest tulenevaid riske ja auditeeritava organisatsiooni riskitaluvust.

4. Auditi kohustus

- 4.1. E-ITS auditi kohustus tuleneb määrusest „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (kehtestatud küberturvalisuse seaduse §7 lõike 5 alusel), E-ITS-i rakendava organisatsiooni eesmärkidest ja lepingulistest kohustustest.
- 4.2. E-ITS audit on soovitatav läbi viia ka organisatsioonidel, kellel auditi kohustust ei ole, kuid kes on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku andmetöötluspartnerid või kelle äriprotsessid on auditi kohuslasega muul viisil seotud.
- 4.3. E-ITS auditi kohustus ei rakendu organisatsioonidele, kelle vastavust standardile ISO/IEC 27001 on nõutud kaitseala osas kinnitatud ISO/IEC 27006 kohaselt akrediteeritud sertifitseerija väljastatud ning kehtiva sertifikaadiga, mis on edastatud järelevalve teostajale (Riigi Infosüsteemi Ametile või julgeolekuasutusele).

5. E-ITS auditi eeldused

- 5.1. Auditi läbiviimise eelduseks on toimiva infoturbe halduse süsteemi olemasolu vastavalt dokumendile „E-ITS Nõuded infoturbe halduse süsteemile” ja E-ITS etaloniturbete meetmete kataloogi viimase 12 kuu jooksul avaldatud versioonile.
- 5.2. Auditi käsitusala on üheselt arusaadavalt piiritletud ja dokumenteeritud.
- 5.3. Infoturbe dokumentatsioon on piisav organisatsiooni infoturbe eesmärkide saavutamiseks ning on vastavuses dokumendiga „E-ITS Nõuded infoturbe halduse süsteemile”.
- 5.4. Auditeeritav on sooritanud järgnevad tegevused:
 - 5.4.1. käsitusalasse kuuluvate äriprotsesside määratlemine;
 - 5.4.2. äriprotsessidega seotud varade kaardistamine;
 - 5.4.3. väliste infoturbealaste nõuete tuvastamine (nt regulatsioonid, lepingud);
 - 5.4.4. kaitsetarbe määramine;
 - 5.4.5. turbeviisi valimine;
 - 5.4.6. modelleerimine (E-ITS moodulite ja meetmete valimine);
 - 5.4.7. riskianalüüsi läbiviimise metoodika kinnitamine;
 - 5.4.8. IT riskianalüüsi läbiviimine (kui vähemalt ühe äriprotsessi kaitsetarve on suurem kui „normaalne”);
 - 5.4.9. infoturbe meetmete rakendusplaani (IMR) koostamine;
 - 5.4.10. infoturbe meetmete rakendamine vastavalt infoturbe meetmete rakendusplaanile;
 - 5.4.11. IT siseauditi või sõltumatute infoturbe läbivaatuste teostamine.
- 5.5. Infoturbe meetmete rakendusplaan sisaldab kõiki modelleerimise käigus tuvastatud asjakohaseid E-ITS turvameetmeid. Väliste turvanõuete määratlemise käigus võib infoturbe

- meetmete rakendusplaani lisada täiendavaid turvameetmeid.
- 5.6. Infoturbe meetmete rakendusplaanis on iga asjakohase meetme kohta sisestatud vähemalt:
- 5.6.1. meetme identifikaator;
 - 5.6.2. meetme nimetus;
 - 5.6.3. meetme teostatuse määr;
 - 5.6.4. meetme rakendamise puhul selgitus, kuidas meede on organisatsioonis rakendatud;
 - 5.6.5. meetme mitterakendamise puhul juhtkonna aktsept meetme mitterakendamisest tulenevatele jääkriskidele või meetme mittekohaldamise põhjendus;
 - 5.6.6. meetme osalise rakendamise puhul täpsustav selgitus, milliste äriprotsesside, varade või alammeetme osas on meede täitmata;
 - 5.6.7. meetme rakendamise eest vastutaja;
 - 5.6.8. meetme rakendamise või meetme järgmise sisulise ülevaatus e tähtaeg.
- 5.7. Infoturbe meetmete rakendusplaani on võimalik esitada meetmete rakendamise hetkeseisu ja plaanitavate tegevusi kajastava tabelina.

6. Auditi üldine korraldus

- 6.1. E-ITS audit koosneb järgmistest auditi etappidest:
- 6.1.1. E-ITS eelaudit (vajadusel);
 - 6.1.2. E-ITS põhiaudit;
 - 6.1.3. E-ITS järelaudit (vajadusel);
 - 6.1.4. E-ITS vaheauditid.
- 6.2. Auditeerimiseks sõlmitakse audiitorettevõttega auditeerimisleping.
- 6.3. Auditeerimislepingu kestvus on üks E-ITS audititsükkel (kolm aastat).
- 6.4. Auditiriski vähendamiseks ei tohi E-ITS audiitor või audiitorettevõtte viia ühes organisatsioonis E-ITS auditeid läbi järjest rohkem kui kahe audititsükli vältel.
- 6.5. Enne auditiprotseduuridega alustamist sõlmitakse audiitorettevõtte ja auditeeritava organisatsiooni vahel konfidentsiaalsusleping.
- 6.6. Auditi läbiviimine plaanitakse koostöös auditeeritava organisatsiooni kontaktsikuga, kes korraldab vajalike isikute olemasolu auditiprotseduuride ajal. Põhjendatud erandjuhtudel tohib auditiprotseduure teostada kaugtöö vormis (sellisel juhul kajastatakse see fakt auditi aruandes).
- 6.7. Enne esmakordset E-ITS auditit või audiitorettevõtte vahetumisel viiakse organisatsioonis esmalt läbi E-ITS eelaudit (p 9 *E-ITS Eelaudit*).
- 6.8. E-ITS põhiauditi läbiviimiseks peavad auditi eeldused (p 5 *E-ITS auditi eeldused*) olema täidetud. Eelauditi käigus audiitori poolt tuvastatud puudused kõrvaldab auditeeritav organisatsioon hiljemalt põhiauditi alguseks.
- 6.9. Kui E-ITS põhiauditi käigus ilmneb kõrge riskitasemega lahknevusi standardist (p 12.7), viiakse kõrge riskitasemega lahknevuste osas läbi järelaudit (p 13. *Auditijärgsed tegevused*).
- 6.10. E-ITS vaheaudit viiakse läbi hiljemalt üks aasta pärast E-ITS põhiauditit või eelmist vaheauditit (p 11. *E-ITS vaheaudit*).
- 6.11. Vaheauditi käigus hinnatakse organisatsioonisiseste (nt äriprotsesse oluliselt mõjutavate IT-süsteemide juurutamine või infoturbe kaitseala laiendamine) ja väliskeskkonnast tulenevate (nt muutuv geopoliitiline olukord või regulatsioon) muutuste mõju organisatsiooni infoturbele.

7. E-ITS auditi tellimine

- 7.1. E-ITS auditi läbiviimise vajadusest teatatakse E-ITS audiitorile või audiitorettevõttele üldjuhul vähemalt kaks kuud ette. Järelauditi ja vaheauditite tellimine ja läbiviimine võib

- pooltevahelisel kokkuleppel toimuda ka lühema etteteatamistähtajaga.
- 7.2. E-ITS auditi tellimisel kirjeldab tellija üheselt ja arusaadavalt auditi käsitusala, sealhulgas auditeerimisele määratud äriprotsesse ja nende kaitsetarvet ning erisusi.
 - 7.3. Tellija esitab rakendatavate E-ITS etaloniturbe moodulite nimekirja, andmetöötluse asukohad ja kasutatavad töökeeled, arvutikasutajate arvu, infoturbe meeskonna ja IT-meeskonna suuruse.
 - 7.4. Kui käsitusalasasse kuuluvaid andmeid töödeldakse mitmes erinevas asukohas, esitab E-ITS auditi tellija hankekutses ja lepingus minimaalse asukohtade arvu, milles audit läbi viiakse. Asukohtade valik ja asukohtade arv peab tagama kõikide asukohatüüpide proportsionaalse esindatuse. Kui andmeid töödeldakse kolmes või vähemas erinevas asukohas (välja arvatud pilvteenuse tarnija asukohad), viiakse auditiprotseduurid läbi kõigis asukohtades.
 - 7.5. Tellija toob hankekutses eraldi välja, kui asukohas kohapealseid auditiprotseduure pole võimalik läbi viia (nt õigusaktidest või teenuseandjaga sõlmitud kokkulepetest tulenevalt).
 - 7.6. E-ITS auditi tellija võib tellida E-ITS auditeid korraga rohkem kui ühele auditeeritavale organisatsioonile. Kui ühe haldusala organisatsioonid tuginevad samale infoturbe halduse süsteemile (nt on neil ühine infoturbe organisatsioon, infoturvapoliitika ja infoturbe dokumentatsioon), võib ühe auditi käsitusala laiendada mitmele organisatsioonile.
 - 7.7. Kui organisatsioon tellib E-ITS auditit mitmendat korda, lisab ta hankekutsele kehtiva auditi järeldusotsuse.
 - 7.8. Tellija võib hankekutses esitada oma nägemuse auditi töömahule.
 - 7.9. Hankekutse põhjal peab E-ITS audiitoril või audiitorettevõttel olema võimalik adekvaatselt hinnata auditiprotseduuride läbiviimisega seotud tööaega ja kulusid. E-ITS auditi hinnastamisel tugineb audiitorettevõtte auditi tellija poolt punktide 7.2 - 7.8 kohaselt esitatud teabele.
 - 7.10. E-ITS järelauditi, täiendavate E-ITS vaheauditite ning käsitusala olulisest muutumisest tingitud lisatööde tellimine toimub auditeerimislepingus kokkulepitud tingimuste ja kehtiva audiitori tunni- või päevahinna alusel.
 - 7.11. Auditi tellimisel tuleb määratleda auditeeritava(te) organisatsiooni(de) kontaktisikud.

8. Nõuded E-ITS audiitorile

- 8.1. E-ITS auditi viib läbi vastava kutseoskusega juhtaudiitor, kes juhib auditirühma tööd, vastutab auditi käigus teostatavate tööde eest ja kes allkirjastab auditi lõppraporti.
- 8.2. Juhtaudiitoril on auditi läbiviimise aja vältel vähemalt üks kehtiv sertifikaat järgnevatest:
 - 8.2.1. Infosüsteemide sertifitseeritud audiitori CISA (*Certified Information Systems Auditor*, CISA) sertifikaat, mille väljaandjaks on ISACA;
 - 8.2.2. ISO 27001 juhtiva audiitori sertifikaat, mille väljaandjaks on IRCA (*International Register of Certificated Auditors*);
 - 8.2.3. ISO 27001 juhtiva audiitori sertifikaat, mille väljaandjaks on PECB (*Professional Evaluation and Certification Board*).
- 8.3. Juhtaudiitor on auditile eelneva kolme kalendriaasta jooksul osalenud vähemalt kolmes infoturbe halduse süsteemi auditis (sh E-ITS ja ISKE auditid). Juhtaudiitoril on vähemalt nelja-aastane IT auditi, IT juhtimise või infoturbe alane töökogemus.
- 8.4. Auditi läbiviimisesse võib kokkuleppel tellijaga kaasata teisi audiitoreid ja tehnilisi eksperte. Kaasatud audiitorid ja eksperdid töötavad juhtaudiitori koordineerimisel.
- 8.5. Auditirühma kaasatud audiitoritel on vähemalt kahe-aastane IT auditi, IT juhtimise või infoturbe alane töökogemus.
- 8.6. Auditirühma kaasatud tehnilistel ekspertidel on auditeerimisobjekti spetsiifikast tulenev tehniline kvalifikatsioon või vähemalt kahe-aastane IT halduse või infoturbe alane töökogemus.

- 8.7. Auditirühma liikmed (juhtaudiitor, teised audiitorid ja kaasatud eksperdid) peavad olema auditeeritavast organisatsioonist sõltumatud ja ei tohi olla osalenud auditeeritava organisatsiooni infoturbe halduse süsteemi kavandamises või rakendamises, sh organisatsiooni konsulteerimises auditeeritavas valdkonnas, auditi alguskuupäevale eelneva kolme aasta jooksul.
- 8.8. Auditirühma liikmete sõltumatus peab olema kinnitatud vastava isiku poolt allkirjastatud deklaratsiooniga.
- 8.9. Auditirühma liikmed peavad tagama oma kohustuste täitmise käigus teatavaks saanud informatsiooni konfidentsiaalsuse. Organisatsiooni poolt sisendina antud isikuandmete töötlemisel, sh isikuandmeid sisaldavate dokumentide läbivaatusel ja logiandmete ja tuvastussüsteemide andmete kasutamisel, järgib audiitor andmekaitsealaste õigusaktide nõudeid.
- 8.10. Audiitor peab auditi läbiviimisel järgima tunnustatud auditeerimise standardeid ja suuniseid, infoturbe parimaid tavaid ja audiitori kutse-eetika koodeksit (nt ISACA <https://eisay.ee/kutse-eetika-koodeks>).
- 8.11. E-ITS audiitor juhendab auditi kavandamisel ja läbiviimisel E-ITS nõuetest ja käesolevast auditeerimisjuhendist. Auditi protseduuride teostamisel järgitakse etalonturbe kataloogi moodulis “DER.3.2 Infoturbe vastavusauditid” esitatud meetmeid.
- 8.12. E-ITS auditi kavandamisel ja auditi maksumuse hindamisel peab audiitor pakkumuses eraldi välja tooma auditi ettevalmistamise, dokumentatsiooni läbivaatuse, kohapealsetele auditiprotseduuride läbiviimise, tõendusmaterjalide analüüsimise ning aruannete koostamisega seonduva töömahu hinnangu ja ajaplaani. Soovitav on anda ka auditeeritava töömahu hinnang.

9. E-ITS eelaudit

- 9.1. Eelaudit viiakse läbi enne esmakordset E-ITS auditit või audiitorettevõtte vahetumisel.
- 9.2. Eelauditi raames hindab audiitor, kas auditeeritav organisatsioon on täitnud auditi eeldustena käsitletavat nõudeid (p 5 *E-ITS auditi eeldused*) või on suuteline täitma auditi eeldused hiljemalt E-ITS põhiauditi alguseks.
- 9.3. Audiitor toob E-ITS eelauditi aruandes välja puudused ning esitab soovitusel auditi eeldustena käsitletavate toimingute sooritamiseks.
- 9.4. Eelauditi käigus audiitori poolt tuvastatud puudused kõrvaldab auditeeritav organisatsioon hiljemalt põhiauditi alguseks.
- 9.5. E-ITS eelauditi ja E-ITS põhiauditi vaheline ajavahemik on maksimaalselt kuus kuud.
- 9.6. Eelauditi aruandele ei rakendata lõpparuande sisule ja vormistamisele kehtivaid nõudeid (p 12 *Lõpparuanne ja järeldusotsus*).

10. E-ITS põhiaudit

- 10.1. Põhiaudit viiakse läbi iga kolme aasta tagant.
- 10.2. Enne põhiauditi läbiviimist koostatakse ja kooskõlastatakse auditeeritava organisatsiooniga auditi plaan.
- 10.3. Audiitor hindab auditi käigus rakendatud infoturbe meetmete ja infoturbe dokumentatsiooni aja- ja asjakohasust ning vastavust Eesti infoturbestandardile.
- 10.4. Infoturbe meetmete rakendusplaanis esitatud põhimeetmete rakendatust kontrollib audiitor täies ulatuses.
- 10.5. Standard- ja kõrgmeetmete rakendamise kontrollimisel lähtub audiitor:
- 10.5.1. äriprotsesside kaitsetarbest ja valitud turbeviisist;
 - 10.5.2. mooduliga seotud ohtude olulisusest organisatsiooni kontekstis;

- 10.5.3. auditeeritava organisatsiooni riskianalüüsi tulemustest;
- 10.5.4. organisatsioonis toimunud infoturbe intsidentidest;
- 10.5.5. varasemate infoturbe auditite leidudest ja läbivaatuste aruannete tähelepanekutest ning soovitudest.
- 10.6. Audiitor lähtub oma hinnangutes riskipõhisuse printsiibist. Üks audiitori tähelepanek võib põhineda ühe või mitme meetme mitterakendamisel või nende osalise rakendamise koosmõjul.
- 10.7. Audiitor viib hinnangu kujundamiseks läbi meetmete toimimise teste, vaatlusi, ringkäike, dokumentatsiooni läbivaatuseid ning intervjuusid.
- 10.8. Auditi tõendusmaterjali võib auditeeritav audiitorile kas väljastada, kohapeal näidata või demonstreerida intervjuu käigus (nt võrguskeem, logide analüsaator, tulemüüri reeglid, õiguste süsteemi selgitamisel reaalsed isikupõhised näited).
- 10.9. Kui dokumentidega tutvumine toimub kohapeal, tagatakse audiitorile selleks vajalik töökoht ja töötingimused.
- 10.10. Auditeeritava organisatsiooni teenuseandjate infoturbe hindamisel võib audiitor oma hinnangu kujundamisel tugineda teenuseandja (nt pilvteenuse tarnija) esitatud auditi käsitusala hõlmavatele ja turvameetmete rakendatust kinnitavatele sertifikaatidele ning vastavusauditite aruannetele.
- 10.11. E-ITS põhiaudit lõpeb auditi lõpparuande ja järelausotsuse esitamisega (p 12 *Lõpparuanne ja järelausotsus*).

11. E-ITS vaheaudit

- 11.1. Kolmeaastase audititsükli jooksul viiakse läbi vähemalt kaks E-ITS vaheauditit.
- 11.2. E-ITS vaheaudit viiakse läbi mitte rohkem kui 12 kuu möödumisel eelmisest auditist (arvestades auditi järelausotsuse või eelmise vaheauditi tulemuste esitamise ajast). Kui organisatsiooni infoturbe kaitsealas on toimunud olulisi muudatusi (nt pärast äriprotsesse oluliselt mõjutavate IT-süsteemide juurutamist või kaitseala laiendamist), tellitakse audit enne plaanitud tähtaega.
- 11.3. E-ITS vaheauditi käigus hindab audiitor:
 - 11.3.1. E-ITS põhiauditi käigus tuvastatud lahknevuste käsitlemist;
 - 11.3.2. infoturbe meetmete rakendusplaani täitmist ning rakendusplaanis tehtud muudatusi;
 - 11.3.3. organisatsioonis toimunud muudatuste mõju infoturbele;
 - 11.3.4. organisatsiooni vastupanuvõimet uutele infoturbe ohtudele;
 - 11.3.5. eelmise põhi- või vaheauditi väljajätte;
 - 11.3.6. E-ITS viimases kehtivas versioonis tehtud muudatuste käsitlemist.
- 11.4. Vaheauditite kavandamise etapis teavitab auditeeritav organisatsioon E-ITS audiitorit muudatustest organisatsiooni äriprotsessides, IT-süsteemides tehtud muudatustest ja toimunud infoturbe intsidentidest.
- 11.5. E-ITS vaheauditi käigus tehtud tähelepanekud vormistab audiitor vaheauditi aruandena lähtudes lõpparuande ja järelausotsuse nõuetest (vt p 12).
- 11.6. E-ITS vaheauditi tulemuste põhjal on audiitoril õigus auditi järelausotsust muuta, esitades selleks organisatsiooni juhtkonnale uue järelausotsuse. Eelmine järelausotsus kaotab seeläbi oma kehtivuse.

12. Lõpparuanne ja järelausotsus

- 12.1. Lõpparuanne koosneb kahest eraldi digiallkirjastatud elektroonilisest dokumendist: auditi järelausotsus ja auditi lõpparuanne.

- 12.2. Auditi järeldusotsus sisaldab:
- 12.2.1. auditeeritava ja audiitori nime;
 - 12.2.2. auditi läbiviimise aega;
 - 12.2.3. käsitusala määratlust;
 - 12.2.4. valitud E-ITS turbeviisi;
 - 12.2.5. audiitori üldhinnangut organisatsiooni infoturbe halduse süsteemi toimimisele.
- 12.3. Auditi järeldusotsus ei sisalda konfidentsiaalset teavet. Auditeeritav organisatsioon tohib auditi järeldusotsust jagada kolmandatele osapooltele.
- 12.4. E-ITS põhiauditi lõpparuanne koosneb järgmistest osadest:
- 12.4.1. auditi kokkuvõte, mis sisaldab audiitori nime, auditi läbiviimise aega, auditi tulemuste lühikokkuvõtet ning audiitori üldhinnangut infoturbe halduse süsteemi toimimisele. Auditi kokkuvõttes esitatakse ka auditi käigus kinnitust saanud positiivsed aspektid;
 - 12.4.2. auditi käsitusala (sh loend auditeeritud äriprotsessidest), äriprotsesside kaitsetarve ja valitud turbeviis (põhiturve, standardturve või tuumikuturve);
 - 12.4.3. auditi meetodika, ajaplaan, auditi läbiviimise kohad ja esinenud piirangud auditi läbiviimisel;
 - 12.4.4. loetelu auditis osalenud auditeeritava organisatsiooni töötajatest ja auditirühma liikmetest ning nende rollide kirjeldused;
 - 12.4.5. audiitori hinnang IT riskide haldusele;
 - 12.4.6. audiitori hinnang infoturbe meetmete rakendamisele;
 - 12.4.7. audiitori hinnang infoturbe halduse süsteemi toimimisele (vähemalt p.12.5 esitatud lõikes);
 - 12.4.8. auditi käigus tuvastatud leiud koos lahknevuste kirjelduste ja riskihinnangutega.
 - 12.4.9. auditi lõpparuande lisadena vormistatud tõendusmaterjal.
- 12.5. Infoturbe halduse süsteemi hindamisel arvestab audiitor vähemalt järgmisi aspekte:
- 12.5.1. kas ISMS vastab dokumendile „E-ITS Nõuded infoturbe halduse süsteemile”;
 - 12.5.2. kas infoturbe eest on määratud vastutajad ja infoturbele on eraldatud piisavad ressursid;
 - 12.5.3. kas kaitseala ja äriprotsessidega seotud varad on määratud piisava detailsuse ja täpsusega;
 - 12.5.4. kas äriprotsesside kaitsetarve on määratud asjakohaselt, tuginedes organisatsiooni poolt antud sisendile regulatsioonide, lepingute ja äriprotsessidest tulenevate nõuete kohta (sh hinnatakse kaitsetarve ülevaatamise sagedust ja protseduure);
 - 12.5.5. kas turbekontseptsiooni teostus, sh valitud turbeviis ja meetmete rakendamine, vastab organisatsiooni vajadustele ja E-ITS nõuetele.
- 12.6. Aruandes tuuakse rõhutatult välja standardist lahknevused:
- 12.2.1. millest tulenevad ühele või mitmele äriprotsessile kõrge tasemega riskid;
 - 12.2.2. mille riskitase üksikult võttes on madal, kuid mis koosmõju tõttu võivad ebasoodsatel asjaoludel kokkusattumisel põhjustada kõrge riski ühele või mitmele äriprotsessile.
- 12.7. Audiitor analüüsib meetmete mitterakendamise põhjendusi ning hindab meetmete mitterakendamisest või osalisest rakendamisest tulenevaid riske järgnevalt:
- Kõrge risk** - oluline lahknevus meetmetes kirjeldatu ja tegeliku olukorra vahel. Meetmete mitterakendamisest tulenevate riskide realiseerumisel võib tekkida suur kahju organisatsiooni varadele ja tegevusele. Kahju toime põhjustab lepingute ja regulatsioonide nõuete rikkumisi, võib ähvardada äriprotsesside jätkusuutlikkust või organisatsiooni olemasolu.
- Madal risk** - osaline lahknevus meetmetes kirjeldatu ja tegeliku olukorra vahel. Riskide realiseerumisel võib tekkida piiratud ja ohjatatav kahju organisatsiooni varadele ja tegevusele nagu lühiajalised töökatkestused.

- 12.8. Et vältida audititsükli jooksul tekkida võivat nõustamise ja auditeerimise konflikti, ei esita audiitor standardi lahknevuste dokumenteerimisel meetme rakendamiseks või lahknevuste kõrvaldamiseks konkreetseid soovitusi.
- 12.9. E-ITS põhiauditi lõpparuandes esitatakse aruande lisadena tõendusmaterjal järgmiste asjaolude kohta:
- 12.9.1. põhiauditi käigus tehtud intervjuude, analüüsitud juhendite, protseduurireeglite jms loend, mille alusel audiitor hinnangu andis;
- 12.9.2. põhiauditi käigus tehtud testimiste ja kontrolliprotseduuride tööpaberid või vaatlustulemused, mis sisaldavad vähemalt tõendusmaterjali:
- varunduse ja taaste toimimise kohta;
 - logimise ja logianalüüsi toimumise kohta;
 - pääsuõiguste halduse toimimise kohta;
 - ründetuvastuse lahenduse toimivuse kohta;
 - intsidendihalduse toimimise kohta;
 - kasutajakoolituste kohta;
 - teenuste väljasttellimise ja partnerasutuste lepingunõuetest tuleneva turbe seire kohta;
 - füüsilise turbe meetmete toimimise kohta.
- 12.10. E-ITS põhiauditi lõpparuande lisana esitatud tööpaberid on kontrollitavad, viited tõendusmaterjalile on piisavad ja testid korratavad.
- 12.11. Kui audiitor on oma töös osaliselt tuginenud varasema E-ITS või ISO27001 auditi tulemustele, tuuakse auditi aruandes selgelt välja, mis osas ning millisele auditi aruandele audiitor on tuginenud.
- 12.12. Enne lõpparuande kinnitamist esitatakse auditeeritava organisatsiooni esindajale auditi aruande kavand. Audiitori tähelepanekutes esinevate ebatäpsuste korrigeerimiseks ja täiendavate tõendusmaterjalide esitamiseks on auditeeritaval organisatsioonil aega vähemalt viis tööpäeva.
- 12.13. E-ITS põhiauditi lõpparuanne esitatakse hiljemalt üks kuu pärast audititoimingute lõpetamist.
- 12.14. Auditeeritav organisatsioon kinnitab kirjalikult taasesitatavas vormis auditi tulemuse vastuvõtmise.
- 12.15. Kokkuleppel tellijaga võib audiitor tutvustada E-ITS põhiauditi lõpparuannet organisatsiooni juhtkonnale, koguda auditi läbiviimise kohta tagasisidet või leppida kokku täiendavate auditite läbiviimise.
- 12.16. Auditeeritava organisatsiooni esindajal on õigus esitada audiitori hinnangu või järeldusotsuste kohta audiitorile kirjalikult taasesitatavas vormis protest. Protestiga arvestamisel viib audiitor auditi aruandesse või järeldusotsusesse sisse asjakohased parandused. Protesti mitteaktsepteerimisel lisab audiitor auditi aruande juurde protesti ja selle mitteaktsepteerimise põhjenduse.
- 12.17. Auditi järeldusotsuse huvitatud osapooltele või auditi aruande ja järeldusotsuse järelevalveasutusele esitab auditi tellija.

13. Auditijärgsed tegevused

- 13.1. Auditeeritav organisatsioon kavandab tegevused parandusmeetmete rakendamiseks, määrab vastutajad ja tähtajad. Infoturbe eest vastutav isik teeb parandusmeetmete rakendamise ülevaatus ja vajadusel ajakohastab infoturbe meetmete rakendusplaani.
- 13.2. Raportis esitatud madala riskitasemega lahknevused (kirjeldatud p 12.7) kõrvaldab auditeeritav organisatsioon mõistliku aja jooksul, kuid mitte hiljem kui audititsükli lõpuks.
- 13.3. Kõrge riskiastmega lahknevused (kirjeldatud p 12.7) on auditeeritav organisatsioon kohustatud kõrvaldama mitte hiljem kui kuue kuu jooksul.

- 13.4. Kõrge riskiastmega lahknevuste osas tellib auditeeritav organisatsioon järelauditi. E-ITS järelauditi tellimist käsitleb p 7 *E-ITS auditi tellimine*.
- 13.5. Kui auditi aruannete säilitustähtaja pikkus ei tulene muudest õigusaktidest või eeskirjadest, säilitab auditi tellija E-ITS auditi aruandeid turvaliselt vähemalt seitse aastat.
- 13.6. Audiitor säilitab auditi aruandeid ja seonduvaid tööpabereid turvaliselt, vastavalt poolte vahelisele kokkuleppele. Juurdepääs dokumentidele on lubatud üksnes vastava pääsuõigusega isikutel.

14. Seonduvad dokumendid

- E-ITS Nõuded infoturbe halduse süsteemile
- E-ITS Rakendusjuhend
- E-ITS Riskihaldusjuhend
- Eesti infoturbestandard. Etalonturbe kataloog. ISMS. Turbehaldus
- Eesti infoturbestandard. Etalonturbe kataloog. DER. Avastamine ja reageerimine
- Infosüsteemide audiitorkontrolli eeskirjad, <https://eisay.ee/infosusteemide-auditorkontrolli-eeskirjad>
- Kutse-eetika koodeks, <https://eisay.ee/kutse-eetika-koodeks>