

Auditeerimiseeskiri

1. Sissejuhatus

1.1. Käesolev auditeerimiseeskiri annab juhiseid määruse lisas 1 toodud infoturbe halduse süsteemi nõuete (edaspidi *infoturbehalduse süsteemi nõuded*) ja lisas 2 toodud etalonturbe kataloogi (edaspidi *etalonturbe kataloog*) (edaspidi koos ka *E-ITS*) auditi (edaspidi *E-ITS audit*) läbiviimiseks. E-ITS auditi läbiviimise kohustusega ja selle läbiviimisest vabastatud organisatsioonid on toodud Vabariigi Valitsuse 09.12.2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *määrus nr 121*) §-s 4.

1.2. Auditeerimiseeskiri on mõeldud E-ITS auditi läbiviijale, E-ITS auditi tellijale ja auditeeritavale organisatsioonile. Auditeeritav organisatsioon saab eeskirja põhjal ülevaate auditi läbiviimise eeldustest, auditi hanke ettevalmistamisest, kohustustest auditi käigus ja auditi kvaliteedi hindamisest. Audiitorile annab eeskiri juhised auditi kavandamiseks, läbiviimiseks ja aruande vormistamiseks.

2. Mõisted ja lühendid

Nr	Mõiste	(inglise/saksa)	Mõiste seletus
1	audiitor	<i>auditor</i>	E-ITS auditit läbi viiv isik, auditirühma liige
2	auditeeritav	<i>auditee</i>	Auditeeritav organisatsioon või selle osa, mida auditeeritakse
3	audiitorettevõtte	<i>auditing entity</i>	Auditeerimislepingu alusel E-ITS auditit läbi viiv ettevõtte (vt p 6)
4	auditirühm	<i>audit team</i>	Audiitoritest ja tehnilistest ekspertidest koosnev rühm auditi läbiviimiseks
5	audititsükkel	-	Määruse nr 121 § 4 lõikest 1 tulenev E-ITS auditeerimisperiood - kolm aastat
6	E-ITS audit	-	E-ITSi põhine sõltumatute pädevate isikute sooritatav süstemaatiline, sõltumatu ja dokumenteeritud protsess infoturbe halduse süsteemi ja infoturbe protsesside läbivaatuseks, tõendite kogumiseks, tõendite objektiivseks hindamiseks ja tulemuste teatamiseks auditeeritavale
7	juhtaudiitor	<i>lead auditor</i>	E-ITS audiitor, kes juhib auditirühma tööd, vastutab auditi läbiviimise eest ja allkirjastab auditi aruanded. Juhtaudiitoril on olemas auditi läbiviimiseks vajalik kvalifikatsioon (vt p 8)

8	kaitsetarve	<i>protection requirement/ Schutzbedarf</i>	vara väärtusest tulenev vajadus seda kaitsta. Kaitsetarve on andmete ja teabe vajadus kaitsta neid kahju eest, mille võib tekitada konfidentsiaalsuse, tervikluse või käideldavuse või kõigi kolme rikkumine. Kaitsetarvet väljendatakse kolmeastmelises skaalas: „normaalne“, „suur“ või „väga suur“
9	käsitlusala	<i>scope</i>	Auditi kontekstis: auditi käsitlusalasse kuuluvad äriprotsessid ja sihtobjektid
10	lahknevus	<i>nonconformity</i>	Erinevus E-ITSi 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 määruse lisas 1 toodud infoturbe halduse süsteemi nõuetega ning on piisavad organisatsiooni äriprotsesside kaitseks ja organisatsiooni eesmärkide täitmiseks.

3.2. Audiitori sõltumatu hinnang annab organisatsioonile, selle klientidele ja partneritele teadmise auditeeritava infoturbe halduse süsteemi jätkusuutlikkuse ja infoturbe ohtudele vastupanuvõime osas.

3.3. E-ITS auditi läbiviimisel arvestatakse infoturbe ohtudest tulenevaid riske ja auditeeritava organisatsiooni riskitaluvust.

4. E-ITS auditi kohustus

4.1. Küberturvalisuse seaduse § 3 lõigetes 1 ja 4 nimetatud juriidilise isiku, riigi- või kohaliku omavalitsuse asutuse, hallatava asutuse, riigitulundusasutuse, avalik-õigusliku juriidilise isiku või nende struktuuriüksuse (edaspidi koos *organisatsioon*), millele on E-ITS auditi läbiviimise kohustus ja auditi läbiviimise aeg sätestatakse määruse nr 121 §-s 4.

4.2. E-ITS audit on soovitatav teostada ka ettevõtjal või asutusel, mis ei ole küberturvalisuse seaduse subjekt, kuid mis on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku andmetöötluspartner või mille äriprotsessid on E-ITS auditi läbiviimise kohusega organisatsiooniga muul viisil seotud.

5. E-ITS auditi eeldused

5.1. E-ITS auditi läbiviimise eelduseks on toimiva infoturbe halduse süsteemi olemasolu organisatsioonis.

5.2. E-ITS auditi käsitlusala on üheselt arusaadavalt piiritletud ja dokumenteeritud.

5.3. Infoturbe dokumentatsioon on piisav organisatsiooni infoturbe eesmärkide saavutamiseks ning on vastavuses infoturbe halduse süsteemi nõuetega.

5.4. Auditeeritav on nõuekohaselt sooritanud järgnevad tegevused:

5.4.1. käsitlusalasse 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 (etalonturbe meetme kataloogi moodulite ja meetmete valimine);
- 5.4.7. riskihalduse metoodika koostamine ja kehtestamine;
- 5.4.8. äriprotsessidega seotud infotehnoloogia (edaspidi *IT*) riskide kaalutlemine (IT-riskianalüüsi koostamine);
- 5.4.9. infoturbe meetmete rakendusplaani (IMR) koostamine;
- 5.4.10. infoturbe meetmete rakendamine vastavalt infoturbe meetmete rakendusplaanis esitatud tähtaegadele;
- 5.4.11. infoturbe sõltumatu läbivaatus või läbivaatused.

5.5. Infoturbe meetmete rakendusplaan sisaldab kõiki modelleerimise käigus tuvastatud asjakohaseid etalonturbe kataloogis toodud turvameetmeid. Väliste turvanõuete määratlemise tulemusena võib infoturbe meetmete rakendusplaan sisaldada täiendavaid turvameetmeid.

5.6. Infoturbe meetmete rakendusplaanis on iga meetme kohta sisestatud vähemalt:

- 5.6.1. meetme identifikaator;
- 5.6.2. meetme nimetus;
- 5.6.3. meetme käsitusviis ja teostuse hetkestaatus (meetme teostatuse määr);
- 5.6.4. meetme rakendamise puhul selgitus, kuidas meede on organisatsioonis rakendatud;
- 5.6.5. meetme mitterakendamise aktsepteerimisel kinnitus 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 ülevaatus tähtaeg.

5.7. Infoturbe meetmete rakendusplaan, sh meetmete rakendamise hetkeseis ja plaanitavad tegevused, on masintöödeldaval kujul.

6. E-ITS 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. E-ITS auditi läbiviimiseks sõlmitakse audiitorettevõttega auditeerimisleping.

6.3. Auditiriski vähendamiseks ei tohi E-ITS audiitor või audiitorettevõtte viia ühes organisatsioonis E-ITS auditeid läbi järjest rohkem kui kahe audititsükli vältel.

6.4. Enne auditiprotseduuridega alustamist sõlmitakse audiitorettevõtte ja auditeeritava organisatsiooni vahel konfidentsiaalsusleping.

6.5. E-ITS auditi läbiviimine plaanitakse koostöös auditeeritava kontaktisikuga, kes tagab vajalike andmete ja isikute kättesaadavuse auditiprotseduuride ajal. Põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teostada kaugtöö vormis, sellisel juhul kajastatakse see fakt auditi aruandes. Kaugtöö osakaal ei tohi ületada 30% auditiprotseduurideks kavandatud tundide kogumahust. Erandiks on organisatsioonid, kes kasutavad ainult virtuaalseid töökohti.

6.6. Enne esmakordset E-ITS põhiauditit teostab audiitorettevõtte organisatsioonis E-ITS eelauditi (vt p 9).

6.7. E-ITS põhiaudit (vt p 10) viiakse läbi iga kolme aasta tagant.

6.8. Kui E-ITS põhiauditi käigus ilmneb kõrge riskitasemega lahknevusi E-ITS-ist (vt p 12.7), viiakse kõrge riskitasemega lahknevuste osas läbi E-ITS järelaudit (vt p 13).

6.9. E-ITS vaheaudit (vt p 11) viiakse läbi ja vaheauditi aruanne esitatakse hiljemalt üks aasta pärast E-ITS põhiauditi või eelmise vaheauditi aruande esitamist.

7. E-ITS auditi kavandamine

7.1. E-ITS auditi läbiviimise vajadusest teatab tellija 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 E-ITS auditi käsitusala, sealhulgas auditeerimisele määratud äriprotsesse ja nende kaitsetarvet ning erisusi.

7.3. Tellija esitab auditeeritavas organisatsioonis rakendamisele määratud E-ITS etalonturbe moodulite nimekirja, andmetöötluse asukohad ja kasutatavad töökeeled, arvutikasutajate arvu, IT meeskonna suuruse, IT-taristu lühikirjelduse ja väljast tellitavate IT-teenuste loendi.

7.4. Kui käsitusalasse kuuluvaid andmeid töödeldakse mitmes erinevas asukohas, esitab E-ITS auditi tellija hankekutses ja lepingus minimaalse asukohtade arvu, mille osas E-ITS 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 ei ole 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 vahetab audiitorettevõtet, lisab ta hankedokumentatsiooni E-ITS auditi kehtiva järelalusotsuse.

7.8. Tellija võib hankedokumentatsioonis esitada oma hinnangu auditi eeldatavast töömahust.

7.9. Hankedokumentatsiooni põhjal peab E-ITS audiitoril või audiitorettevõttel olema võimalik adekvaatselt hinnata auditiprotseduuride läbiviimisega seotud tööaega ja kulusid. E-ITS auditi hinna määramisel tugineb audiitorettevõtte punktide 7.2 - 7.8 kohaselt esitatud teabele.

7.10. E-ITS järelauditi ning käsitusala olulisest muutumisest tingitud lisatööde tellimine toimub auditeerimislepingus kokkulepitud tingimuste ja kehtiva audiitori tunni- või päevahinna alusel. Oluliseks muutumiseks loetakse käsitusala laiendamist (nt äriprotsesside arvu suurenemist) rohkem kui 10% ulatuses.

7.11. E-ITS auditi tellimisel tuleb määratleda auditeeritava(te) organisatsiooni(de) kontaktisik(ud).

7.12. E-ITS auditi kavandamisel ja E-ITS auditi maksumuse hindamisel esitab audiitor auditipakkumuses iga auditi etapi juures audiitori töömahu hinnangu ja eeldatava ajaplaani. Soovitav on lisada ka auditeeritava töötajate töömahu hinnang. Põhiauditi töömaht moodustab vähemalt 60% kogu audititsükliks kavandatud audititundide kogumahust, ühe vaheauditit töömaht vähemalt 10% audititsükliks kavandatud audititundide kogumahust.

8. Nõuded E-ITS audiitorile

8.1. E-ITS auditi viib läbi vastava kutseoskusega juhtaudiitor, kes juhib auditirühma tööd, vastutab E-ITS auditi käigus teostatavate tööde eest ja allkirjastab E-ITS auditi lõpparuande ja E-ITS auditi järeldusotsuse.

8.2. Juhtaudiitoril on E-ITS 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 E-ITS auditile eelneva kolme aasta jooksul osalenud audiitorina vähemalt kolmes infoturbe või IT-süsteemide halduse auditis (sh E-ITS ja ISKE auditid). Juhtaudiitoril on vähemalt nelja-aastane IT auditi, IT juhtimise või infoturbe alane töökogemus.

8.4. E-ITS auditi läbiviimisse 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 spetsiifikale vastav 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 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 auditeerimise tunnustatud standardeid ja suuniseid, infoturbe parimaid tavasid ja audiitori kutse-eetika koodeksit (nt ISACA <https://eisay.ee/kutse-eetika-koodeks>).

8.11. E-ITS audiitor juhendub auditi kavandamisel ja läbiviimisel infoturbealalduse süsteemi nõuetest ja käesolevast auditeerimiseeskirjast. Auditi protseduuride teostamisel järgitakse etaloniturb kataloogi moodulis "DER.3.2 Infoturbe vastavusauditid" esitatud meetmeid.

9. E-ITS eelaudit

9.1. E-ITS eelaudit tellitakse ja viiakse läbi organisatsiooni esmakordse E-ITS auditi raames.

9.2. E-ITS eelauditi käigus hindab audiitor, kas auditeeritav organisatsioon on täitnud E-ITS auditi eeldustena käsitletavat nõudet (vt p 5) või on suuteline täitma E-ITS auditi eeldused hiljemalt E-ITS põhiauditi alguseks.

9.3. Audiitor toob E-ITS eelauditi aruandes välja puudused ning esitab soovitusel E-ITS auditi eeldustena käsitletavate toimingute sooritamiseks.

9.4. E-ITS eelauditi aruandes esitatud puudused kõrvaldab auditeeritav organisatsioon hiljemalt E-ITS põhiauditi alguseks.

9.5. E-ITS eelauditi ja E-ITS põhiauditi vaheline ajavahemik on maksimaalselt kuus kuud.

9.6. E-ITS eelauditi aruandele ei rakendata lõpparuande sisule ja vormistamisele kehtivaid nõudeid (vt p 12).

10. E-ITS põhiaudit

10.1. E-ITS põhiauditi läbiviimiseks peavad auditi eeldused (vt p 5) olema täidetud. Eelauditi käigus audiitori poolt tuvastatud puudused kõrvaldab auditeeritav organisatsioon hiljemalt põhiauditi alguseks. Juhul, kui E-ITS auditi eeldused on täitmata, on audiitoril õigus põhiauditi algust edasi lükata.

10.2. Enne E-ITS põhiauditi läbiviimist koostatakse ja kooskõlastatakse auditeeritava organisatsiooniga E-ITS auditi plaan. Auditi plaan aitab tagada, et kriitilistele kontrollivaldkondadele pööratakse auditi käigus piisavalt tähelepanu ja auditiprotseduurid tehakse õiges järjekorras. Olude muutudes või ootamatute asjaolude ilmnedes muudetakse vastavalt ka auditi plaani.

10.3. E-ITS auditi käigus hindab audiitor:

10.3.1. vastavust infoturbe halduse süsteeminõuetele;

10.3.2. infoturbe dokumentatsiooni aja- ja asjakohasust;

10.3.3. infoturbe meetmete asjakohasust, riskipõhisust ning proportsionaalsust.

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

10.5. Infoturbe meetmete rakendusplaanis esitatud meetmete rakendatust, rakendustähtaegade ja väljajätmise asjakohasust ning proportsionaalsust hindab audiitor kõigi rakendamisele kuuluvate etalonturbe kataloogi moodulite osas. Meetmete rakendamist kontrollitakse valikuliselt, vastavalt kinnitatud ajaplaanile. Kontrollitavate meetmete valimisel lähtub audiitor:

10.5.1. äriprotsesside kaitsetarbest ja valitud turbeviisist;

10.5.2. mooduliga seotud ohtude olulisusest organisatsiooni kontekstis;

10.5.3. auditeeritavas organisatsioonis teostatud infoturbe riskide kaalutlemise tulemustest;

10.5.4. organisatsioonis toimunud infoturbe intsidentidest;

10.5.5. varasemate infoturbe auditite leidudest ja läbivaatuste aruannete tähelepanekutest ning soovitustest;

10.5.6. auditeeritavale eelnevalt tutvustatud metoodikast meetmetest valimi moodustamiseks.

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 auditiprotseduure, milleks on intervjuud, meetmete toimimise testid, paikvaatlused ja dokumentatsiooni läbivaatus. Auditiprotseduuride maht on vähemalt 60 % auditi üldisest töömahust.

10.8. E-ITS 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 audiitor tugineb oma hinnangu kujundamisel 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 järeldusotsuse esitamisega (vt p 12).

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 E-ITS auditist, arvestades E-ITS auditi järeldusotsuse või eelmise E-ITS vaheauditi tulemuste esitamise ajast. Kui organisatsiooni infoturbe kaitsealas on toimunud olulisi muudatusi (nt laiendati kaitseala või võeti kasutusele äriprotsesse oluliselt mõjutavad IT-süsteemid), tellitakse E-ITS 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 organisatsiooni infoturbele;

11.3.4. organisatsiooniväliste tegurite muutumise mõju organisatsiooni infoturbele;

11.3.5. eelmise E-ITS põhi- või vaheauditi käsitusala väljajätte;

11.3.6. E-ITS viimases kehtivas versioonis tehtud muudatuste käsitlemist.

11.4. E-ITS vaheauditite kavandamise etapis teavitab auditeeritav organisatsioon E-ITS audiitorit muudatustest organisatsiooni äriprotsessides, IT-süsteemides tehtud muudatustest ja toimunud infoturbe intsidentidest, mis võivad mõjutada vaheauditi käsitusala.

11.5. E-ITS vaheauditi käigus tehtud tähelepanekud vormistab audiitor E-ITS vaheauditi aruandena lähtudes lõpparuande ja järeldusotsuse nõuetest (vt p 12).

11.6. E-ITS vaheauditi tulemuste põhjal on audiitoril õigus E-ITS auditi järeldusotsust muuta, esitades selleks organisatsiooni juhtkonnale uue järeldusotsuse. Eelmine järeldusotsus kaotab seeläbi oma kehtivuse.

12. Lõpparuanne ja järeldusotsus

12.1. Lõpparuanne koosneb kahest eraldiseisvast ja juhtaudiitori poolt digiallkirjastatud elektroonilisest dokumendist: E-ITS auditi järeldusotsus ja E-ITS auditi lõpparuanne.

12.2. E-ITS auditi järeldusotsus sisaldab:

12.2.1. auditi tellija nimetust ja auditi käsitusalas olevate organisatsioonide nimetusi ning registrikode;

12.2.2. E-ITS auditi läbiviimise kestust;

12.2.3. käsitusala määratlust;

12.2.4. valitud E-ITS turbeviisi;

12.2.5. audiitori üldhinnangut organisatsiooni infoturbe halduse süsteemi toimimisele. Üldhinnang sisaldab muuhulgas seda, kas ja kui palju tuvastati auditi käigus kõrge riskitasemega lahknevusi;

12.2.6. audiitorettevõtte ja auditi läbiviinud juhtaudiitori nime.

12.3. E-ITS auditi järeldusotsus ei sisalda konfidentsiaalset teavet. Auditeeritav organisatsioon tohib E-ITS auditi järeldusotsust jagada kolmandatele osapooltele.

12.4. E-ITS põhiauditi lõpparuanne koosneb järgmistest osadest:

12.4.1. E-ITS auditi kokkuvõte, mis sisaldab audiitori nime, auditi läbiviimise aega, E-ITS auditi tulemuste lühikokkuvõtet ning audiitori üldhinnangut infoturbe halduse

süsteemi toimimisele. E-ITS auditi kokkuvõttes esitatakse ka E-ITS auditi käigus kinnitust saanud positiivsed aspektid;

12.4.2. E-ITS auditi käsitusala (sh loend äriprotsessidest), äriprotsesside kaitsetarve ja valitud turbeviis (põhiturve, standardturve või tuumikuturve);

12.4.3. E-ITS auditi metoodika, ajaplaan, auditi läbiviimise kohad ja esinenud piirangud E-ITS auditi läbiviimisel;

12.4.4. loetelu E-ITS 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;

12.4.8. E-ITS auditi käigus tuvastatud leiud koos lahknevuste kirjelduste ja audiitori lisatud riskihinnangutega;

12.4.9. E-ITS auditi lõpparuande lisadena vormistatud tõendusmaterjal.

12.5. Infoturbe halduse süsteemi hindamisel arvestab audiitor vähemalt järgmisi aspekte:

12.5.1. kas see vastab infoturbe halduse süsteemi nõuetele (vt määruse lisa 1);

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 edastatud andmetele regulatsioonide, lepingute ja äriprotsessidest tulenevate nõuete kohta, sealhulgas hinnatakse kaitsetarbe 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 välja auditi leiud ja iga leiuga kaasneva riski mõju äriprotsessile selgitavad riskihinnangud. Leidudena käsitletakse lahknevusi standardist:

12.6.1. millest tulenevad ühele või mitmele äriprotsessile madala tasemega riskid;

12.6.2. millest tulenevad ühele või mitmele äriprotsessile kõrge tasemega riskid;

12.6.3. mille riskitase üksikult võttes on madal, kuid mis koosmõju tõttu võivad asjaolude ebasoodsal 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:

12.7.1. 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 mittetäitmist, võib ähvardada äriprotsesside jätkusuutlikkust või organisatsiooni olemasolu;

12.7.2. Madal risk - väheoluline lahknevus meetmetes kirjeldatu ja tegeliku olukorra vahel. Riskide realiseerumisel võib tekkida piiratud ja ohjatatav kahju organisatsiooni varadele ja tegevusele (nt lühiajalised töökatkestused).

12.8. Audititsükli vältel tekkida võiva nõustamise ja auditeerimise konflikti vältimiseks ei esita audiitor lahknevuste auditeeritavale esitamisel meetme rakendamiseks või lahknevuste kõrvaldamiseks konkreetseid soovitusi.

12.9. E-ITS auditi lõpparuandes esitatakse loend auditi käigus läbiviidud intervjuudest, tuginetud poliitikatest ja juhenditest.

12.10. E-ITS auditi lõpparuandes esitatakse loend auditi käigus kontrollitud E-ITS meetmetest. Kui audiitor on teinud meetmetest valimi, esitatakse täiendavalt valimi koostamise metoodika.

12.11. E-ITS auditi käigus tehtud leidude kohta on audiitoril olemas tõendusmaterjal, auditi testid on korratavad.

12.12. Kui audiitor on oma töös osaliselt tuginenud varasema E-ITS või ISO/IEC 27001 auditi tulemustele, tuuakse auditi aruandes selgelt välja, mis osas ning millisele auditi aruandele audiitor on tuginenud.

12.13. Enne E-ITS auditi lõpparuande kinnitamist esitatakse auditeeritava organisatsiooni esindajale E-ITS auditi aruande kavand. Audiitori tähelepanekutes esinevate ebatäpsuste korrigeerimiseks ja täiendavate tõendusmaterjalide esitamiseks on auditeeritaval organisatsioonil aega vähemalt viis tööpäeva.

12.14. E-ITS põhiauditi lõpparuanne esitatakse hiljemalt üks kuu pärast audititoimingute lõpetamist. Auditeeritav organisatsioon kinnitab E-ITS auditi aruande vastuvõtmise kirjalikult taasesitatavas vormis.

12.15. Kokkuleppel tellijaga võib audiitor tutvustada E-ITS põhiauditi lõpparuannet organisatsiooni juhtkonnale, koguda E-ITS 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 teeb audiitor E-ITS auditi aruandes või järeldusotsuses asjakohased parandused. Protesti mitteaktsepteerimisel lisab audiitor E-ITS auditi aruande juurde protesti ja selle mitteaktsepteerimise põhjenduse.

12.17. Järelevalveasutusele esitab E-ITS auditi aruande ja E-ITS auditi järeldusotsuse E-ITS auditi tellija.

13. Auditijärgsed tegevused

13.1. Auditeeritav organisatsioon kavandab tegevused parandusmeetmete rakendamiseks, määrab vastutajad ja tähtajad. Parandusmeetmete rakendamist ja infoturbe meetmete rakendusplaani ajakohastamist koordineerib infoturbe eest vastutav isik.

13.2. Auditeeritav organisatsioon kõrvaldab raportis esitatud madala riskitasemega lahknevused (vt p 12.7) või määrab lahknevuse käsitlesviisi hiljemalt järgmise auditi alguseks.

13.3. Kõrge riskiastmega lahknevused (vt p 12.7) on auditeeritav organisatsioon kohustatud kõrvaldama mitte hiljem kui kuue kuu jooksul.

13.4. Kõrge riskiastmega lahknevuste kohta tellib auditeeritav organisatsioon E-ITS järelauditi. (vt p 7).

13.5. Kui E-ITS auditi aruannete säilitustähtaeg ei tulene muudest õigusaktidest või eeskirjadest, säilitab auditi tellija E-ITS auditi aruandeid turvaliselt vähemalt seitse aastat.

13.6. Audiitor säilitab E-ITS auditi aruandeid ja seonduvaid tööpabereid turvaliselt, vastavalt poolte vahelisele kokkuleppele. Juurdepääs dokumentidele on lubatud üksnes vastava pääsuõigusega isikul.