„Justiits- ja digiministri PP.KK. 2026
määruse nr „Eesti infoturbestandard“
lisa 2

Auditeerimiseeskiri

1. Terminid ja lühendid

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 – Eesti infoturbestandardi järgimise auditeerimine määruse § 11 lõikes 1 sätestatud eesmärgil;
auditeeritav – (inglise keeles *auditee*) 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 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 auditiaruandes. Kaugtöötunnid ei tohi ületada 30% audititööks kavandatud tundide koguarvust. Erandiks on auditeeritav, kes kasutab ainult virtuaalseid töökohti.

3. Auditi tellimine või hankimine

3.1. Auditit tellides või hankides kirjeldab auditeeritav üheselt ja arusaadavalt auditi käsitlusala, sealhulgas auditeeritavaid äriprotsesse, neile määratud kaitsetarvet ning nende erisusi.

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. Audiitor 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. 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. äriprotsessidele määratud kaitsetarbest;
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 audiitor auditiprotseduure, mille maht moodustab vähemalt 60% audiitori kogutöömahust 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 teenuseandjate infoturbe hindamisel tugineb audiitor oma hinnangut kujundades teenuseandja (nt pilvteenuse tarnija) esitatud auditi käsitlusala hõlmavatele ja turvameetmete rakendatust kinnitavatele sertifikaatidele ning vastavusauditite aruannetele.

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 juhtivaudiitori nimi.

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 neile määratud kaitsetarve;

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 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 äriprotsessidega seotud varad;

6.6.4. organisatsioonis on määratud äriprotsesside nõuetelevastav kaitsetarve;

6.6.5. organisatsioonis on teostatud infoturbe haldus, sh valitud meetmed vastavad organisatsiooni kaitsetarbele.

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 väiksed, 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 meetmetest.

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.

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.

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

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

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