

**JUHEND INFOTURBE HALDUSE SÜSTEEMI AUDIITORTEENUSE RIIGIHANKE KORRALDAMISEKS
OMAAVALITSUSES**

Sisukord

1. Sissejuhatus.....	3
1.1. Eesmärk.....	3
1.2. Normiviited	3
1.3. Mõisted	4
2. E-ITS audit	6
2.1. Auditi õiguslik alus	6
2.2. Audit korraldus ja käik.....	6
3. E-ITS auditi hankimine.....	10
3.1. Riigihanke ese ja riigihanke alusdokumendid	10
3.1.1. Riigihanke ese.....	10
3.1.2 Auditi periood	11
3.2. Tehniline kirjeldus	12
3.3. Eeldatav maksumus.....	13
3.4. Auditi meeskond	13
3.5. Kõrvaldamise alused	14
3.6. Kvalifitseerimistingimused	14
3.7. Hinnatavad näitajad ning pakkumuste hindamine	15
5. Hankeleping	16
6. Muude auditite hankimine.....	17
6.1. ISO 27001 audit.....	17
6.2. Infoturbe siseaudit (ISO 27001 või E-ITS).....	18
6.3. Sõltumatu läbivaatus	18
7. Kokkuvõte.....	19

1. Sissejuhatus

1.1. Eesmärk

Käesoleva soovitusliku juhendi eesmärk on ühtlustada Eesti infoturbe standardi (E-ITS) auditi hankija (edaspidi hankija) ja pakkuja arusaamad, selleks et:

- hankija oskaks riigihanke alusdokumendid sõnastada viisil, mis tagaks asjakohased pakkumised;
- hankija suudaks selgitada ja piiritleda riigihanke alusdokumentides täpselt, missugust auditit ta vajab, mis perioodiks ja milline on auditi käsitusala;
- riigihanke alusdokumentides sätestatud tingimustega ei piirataks põhjendamatult pakkujate hulka ega iga üksikut pakkujat eraldi;
- riigihankes esitatud tingimused ei oleks vastuolus infoturbe auditi üldpõhimõtteid sätestavate standarditega, sh eetikakoodeksiga;
- riigihanke alusdokumendid oleks koostatud viisil, mis võimaldab pakkujatel vältida huvide konflikti ning pakkuda parimat teenust õiglase hinnaga;
- vähendada ja hanke ettevalmistamise ja pakumuse vormistamise töö mahtu.

Juhend lähtub õigusaktidest, mis kehtivad juunis 2025. Juhendi koostamise ajal on juba olemas [KÜTS muutmise eelnõu](#), mille jõustumise aeg ega jõustatav sisu ei ole teada.

Juhend käsitleb E-ITS vastavusauditi hankimist, kuid on asjakohaste sõnastuse muudatustega kasutatav ka E-ITS rakendamise nõustamise hankimisel. Samuti on viimases peatükis lühidalt käsitletud muude asjakohaste auditite hankimise eripärasid.

1.2. Normiviited

- [Küberturvalisuse seadus](#)
- [Vabariigi Valitsuse 09.12.2022 määrus nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded”](#)
- [Ettevõtlus- ja infotehnoloogiaministri määrus 16.12.2022 määrus nr 101 "Eesti infoturbestandard"](#)
- [E-ITS nõuded infoturbe halduse süsteemile](#) versioon 2023
- [EVS-EN ISO 19011:2018](#) Juhtimissüsteemi auditeerimise juhised
- [Auditeerimisjuhend](#) versioon 2023¹
- [E-ITS auditeerimiseeskiri](#) kavand 2024
- [Hädaolukorra seadus](#)

¹ Siin ja edaspidi on dokumendile viidates aluseks juunis 2025 kehtiv auditeerimisjuhend ehk 2023. aasta versioon. Soovitame alati üle kontrollida, kas on kehtestatud uus versioon, kuna muudatused võivad olla olulised.

- [Isikuandmete kaitse üldmääruse \(IKÜM\)](#)
- [Eesti infosüsteemide audiitorite ühing kutse-eetika koodeks](#)
- Riigihangete seadus

1.3. Mõisted

infoturbe halduse süsteem (ISMS, Information Security Management System)

süsteem, mis koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, et kaitsta oma varasid. ISMS on suunatud ärieesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemist infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele. See põhineb riskide kaalutlemisel ja nende aktsepteerimisel tasemele, mis tagavad riskide toimiva käsitlemise ja halduse.

audit

süstemaatiline sõltumatu ja dokumenteeritud [protsess auditi asitõendite](#) saamiseks ja asitõendite objektiivseks hindamiseks eesmärgiga otsustada, mil määral on auditi kriteeriumid täidetud (ISO 9000, ISO 22300, ISO/IEC 27000)

Selgituseks: Mõiste „audit“ all käsitletakse juhendis infoturbe audiitori ja tema meeskonna poolt tehtavaid töid lähtuvalt auditi ülesandest.

vastavusaudit

audit, mis tõendab nõuete täidetust

sertifitseerimisaudit

audit, mille tulemusel väljastatakse sertifikaat nõuetele vastavuse kohta

sertifikaat

standardile, eeskirjale vms [vastavuse](#) tõend

vaheaudit

audit, mis viikase läbi mitte rohkem kui aasta pärast põhiauditit kontrollimaks leitud lahknevuste käsitlemist, rakendusplaani täitmist ning sisemiste ja väliste muudatuste mõju organisatsiooni infoturbele

järeldudit

kõrge riskiastmega lahknevuste kõrvaldamise tulemuste saavutamise audit

täiendav E-ITS vaheaudit

käsitlusala olulisest muutumisest tingitud lisaaudit

ülevaatus

kontrollimine üldpildi (ülevaate) saamiseks, [ISMS](#) kontekstis on pealiskaudsem kui [läbivaatus](#)

läbivaatus

tegevus otsustamiseks, kui sobiv, adekvaatne ja toimiv on läbivaadatav objekt (poliitika, turvameede, protsess) püstitatud [eesmärkide](#) saavutamiseks (ISO 31073, ISO 9000, ISO/IEC 27000 jt)

auditi aruanne

[auditi leidude](#) ning neist tulenevate [järeldeste](#) ja soovitude esitus

järeldusotsus

[auditi](#) tulem pärast auditi eesmärkide ja kõigi [auditi leidude](#) arvessevõttu (ISO 9000, ISO 19011)

audiitor

isik, kes sooritab [auditi](#)

juhtaudiitor

E-ITS audiitor, kes juhib auditirühma tööd, vastutab auditi läbiviimise eest ja allkirjastab auditi aruanded. Juhtaudiitoril on olemas auditi läbiviimiseks vajalik kvalifikatsioon

tehniline ekspert

auditi meeskonna liiga, valdkonnaspetsiifiliste eriteadmiste ja oskustega isik

audiitori sertifikaat

audiitori kutseoskuste nõuetele [vastavuse](#) tõend

audiitorettevõtte

auditeerimislepingu alusel E-ITS auditit teostav ettevõtte

auditi meeskond / auditirühm

audiitoritest ja tehnilistest ekspertidest koosnev rühm auditite läbiviimiseks

auditi programm

[auditiks](#) vajalike tegevuste ja korra kirjeldus. Reeglina pikemaks ajaks, nt auditi tsükliks

auditiplaan

[auditiks](#) vajalike tegevuste ja korra kirjeldus. Reeglina üheks aastaks

lahknevus

erinevus standardi kohalduva osa ja tegeliku olukorra vahel

oluline lahknevus

erinevus standardi kohalduva osa ja tegeliku olukorra vahel, mille tõttu ilmneb kõrge risk

2. E-ITS audit

2.1. Auditi õiguslik alus

Küberturvalisuse seadus (KüTS) sätestab ühiskonna toimimise seisukohast oluliste ettevõtete ja asutuste, sealhulgas avaliku sektori, jaoks võrgu- ja infosüsteemide pidamise nõuded.

KüTS alusel on vabariigi valitsus kehtestanud määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ 09.12.2022 nr 121 [RT I, 13.12.2022, 30](#) (edaspidi VV määrus 121), mis omakorda on volitanud ettevõtluse ja infotehnoloogia ministrit oma määrusega 16.12.2022 nr 101 [RT I, 21.12.2022, 34](#) kehtestama Eesti Infoturbe standardi.

Käesoleva juhendi seisukohalt on esmajoones oluline KüTS § 7, milles sätestatakse kohustus rakendada infoturvameetmed ja VV määrus 121, mis määrab E-ITS rakendamise ja/või auditeerimise kohuslased.

KüTS-st tuleneva kohustuse järgi infoturbe halduse süsteemi rakendanud teenuse osutajatel, sh ka omavalitsustel on Vabariigi Valitsuse 09.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 4 alusel kohustus läbi viia **E-ITS vastavusaudit**.

Sama määrus näeb ette ka alternatiivi E-ITS rakendamisele ning auditeerimisele. Nimelt võib teenuse osutaja rakendada rahvusvahelise standardi ISO/IEC 27001 nõuetele vastavad turvameetmed ning esitada asjakohase sertifikaadi, mille kohaldamisala hõlmab **vähemalt** E-ITSi kohaldamisala.

Kindlasti on mõistlik enne auditi tellimist selgitada välja auditi kohustuse kehtivus viidatud VV määruse 121 §4 järgi, mis ütleb:

(4) Lõikes 1 sätestatud (ehk auditi kohustust) **ei kohaldata:**
1) teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 10 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 2 miljonit eurot (mikroettevõttele);
2) riigimuuseumile, avalik-õigusliku isiku muuseumile, valla või linna ametiasutusele, valla või linna ametiasutuse hallatavale asutusele, osavalla või linnaosa ametiasutusele, osavalla või linnaosa ametiasutuse hallatavale asutusele ning kohaliku omavalitsuse üksuste ühisametile ja -asutusele, kui **tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga**.

NB! Seejuures ei vabasta auditi kohustusest „pääsemine“ infoturbe meetmete ehk E-ITS rakendamisest.

Käesolev juhend käsitleb esmajoones E-ITS auditi tellimist.

2.2. Audit korraldus ja käik

Auditi hankimise juhised tulenevad suuresti auditi olemusest ning korraldusest. Sellepärast on asjakohane alustada põgusa ülevaatega auditi korraldusest ning käigust.

E-ITS auditi saab hankija vaates jagada järgmisteks peamisteks etappideks:

- auditi ettevalmistus,
- algatamine (tihti avakoosoleku vormis),

- eelaudit,
- ettevalmistus põhiauditiks,
- põhiaudit,
- auditi kokkuvõtted,
- järelaudit (vajadusel),
- täiendav E-ITS vaheaudit (vajadusel),
- vaheauditid.

Igal etapil on mõlemal poolel – auditeeritaval ja audiitoril - oma ülesanded.

Auditi ettevalmistuse faasis loob hankes edukaks tunnistatud audiitorfirma oma meeskonna kooskõlas hanke nõuete ja pakkumisega.

Oluline roll meeskonnas on juhtaudiitoril, kes vastutab auditi hea läbiviimise eest kogu selle vältel (ISO 19011 p 6.2.1). Auditi meeskonnas võivad olla veel audiitorid ja tehnilised eksperdid.

Juhtaudiitori ülesanneteks on:

- auditi teostatavuse hinnang,
- auditi plaani koostamine,
- auditi riskide haldus,
- suhtlus auditeeritavaga,
- auditimeeskonna juhtimine ja ülesannete jagamine,
- erimeelsuste lahendamine,
- aruande ja järeldusotsuse koostamine ja allkirjastamine.

Avakoosoleku eesmärgiks on tutvuda auditeeritava ja auditi meeskondadega ning kokku leppida töö põhimõtted auditi käigus – eeldatav tööde järjekord, dokumentide ja muu asjakohase teabe vahetamise viisid.

Esmakordsel E-ITS auditi järgneb avakoosolekule **eelaudit**, mille käigus audiitor hindab, kas auditeeritav organisatsioon on täitnud E-ITS auditi eeldustena käsitletavat nõudet. Eeldused on loetletud E-ITS auditeerimisjuhendi vastavas peatükis. Auditeerimisjuhend näeb ette eelauditi korraldamise lisaks esmakordsele auditeerimisele ka juhul, kui vahetub audiitor.

Eelauditiks esitab auditeeritav audiitorile kõik tõendused E-ITS auditeerimisjuhendi peatükis 5 loetletud nõuete kohta. Need on kas dokumendid (nt poliitikad, teemapoliitikad, meetmete rakendusplaan) või viited dokumenteeritud teabele, mis tõendaks vajalike protsesside toimivust.

Audiitoril on kogu auditi käigus õigus ja kohustus paluda lisainformatsiooni, et olla kindel halduse süsteemi nõuetele vastavuses. Audiitor ei saa oma töös tugineda ainult suulistele väidetele, vaid vajab tõendusmaterjali. Audiitor lähtub riskipõhiselt tõendusväärtusest järgmiselt: alates väiksema tõendusväärtusega suulistest ütlustest ja edasi kirjalikest dokumentidest, vaatlustest kuni testide ja kirjade ülevaatuseni.

Audit saab alata, kui hankijal on olemas lõplik info audiitorile esitamiseks.

Audiitor hindab veel auditeeritava üldist lähenemist ja arusaamist infoturbe halduse süsteemi toimimisest, täpsustab põhiauditi plaani ja tutvub eelnevate auditite aruannetega.

Eelauditi järel esitab audiitor eelauditi aruande, milles toob välja puudused ning esitab soovitused. Eelauditi käigus audiitori poolt tuvastatud puudused kõrvaldab auditeeritav hiljemalt E-ITS põhiauditi alguseks.

Põhiauditiks ettevalmistuse käigus koostab juhtaudiitor E-ITS põhiauditi (E-ITS auditeerimisjuhendi peatükk 10) plaani.

Esialgne plaan, mis esitatakse tihti pakkumise koosseisus, ei saa olla väga üksikasjalik, sest nii hanked kui auditid on täis ootamatusi. Lisaks ei avalda auditeeritav hanke alusdokumentides kogu konfidentsiaalset teavet (nt riskiregistri sisu) infoturbe halduse süsteemist.

Auditi plaan koostatakse eeldusel, et auditeeritav on infoturbe halduse süsteemi rakendamisega valmis ja seega ka auditiks valmis. Eelauditi ja põhiauditi vaheline ajavahemik on maksimaalselt kuus kuud.

Juhtaudiitor tutvustab plaani E-ITS eelauditi järel ja vajadusel räägitakse see läbi osapoolte vahel. Oodatava ajastuse korral peab hankija arvestama piisava ajavaruga audiitorteenuse protseduuride tegemiseks.

Juhtaudiitor plaanib tegevused reeglina ühtse töövoona võimalikult väheste katkestustega. Infoturbe halduse süsteemi eri osade auditiks esitamisega viivitamine ei ole põhjendatud ja tekitab olulisi ebamugavusi mõlemale osapooltele.

Samas ei ole alust eeldada, et audiitor lõpetab protseduurid väga lühikese aja jooksul pärast seda, kui hankija on materjalid esitanud. Palju sõltub auditeeritava valmisolekust leida asitõendeid, mida audiitor küsib, leidmaks kinnitust nõuete täitmise kohta.

Põhiauditi käigus audiitor kontrollib;

- teavet ja tõendeid halduse süsteemi vastavusest kõikidele kehtivatele standardi ja muude normdokumentide nõuetele;
- halduse süsteemi eesmärkide saavutamise tulemuslikkuse seiret, mõõtmist, aruandlust ja ülevaatamist;
- kliendi suutlikkust täita toimiva juhtimissüsteemi abil kehtivate seaduste, regulatiivsete ja lepinguliste kohustuste nõudeid;
- protsesside operatiivset haldust;
- siseauditi ja juhtkonnapoolsete ülevaatuste tõhusust;
- juhtkonna eestvedamist.

E-ITS auditi lõpparuanne koosneb kahest eraldi digiallkirjastatud elektroonilisest dokumendist:

- E-ITS auditi järelendusotsus ja
- E-ITS auditi lõpparuanne.

Aruande koostamisel lähtub audiitor järgmistest põhimõtetest:

- a) aruande koostamisel lähtutakse Eesti infoturbe standardist;
- b) kui auditeeritavaid asutusi on mitu, siis koostatakse auditi aruanne iga asutuse kohta eraldi.

Auditi aruande esmane kavand esitatakse enne E-ITS lõpparuande kinnitamist auditeeritava organisatsiooni esindajale, misjärel antakse (küll mitte pikk) aeg audiitori tähelepanekutes esinevate ebatäpsuste korrigeerimiseks ja täiendavate tõendusmaterjalide esitamiseks.

Järelaudit tehakse vaid juhul, kui auditi aruandes on toodud kõrge riskiastmega lahknevused. Sellised lahknevused peab auditeeritav kõrvaldama kuue kuu jooksul, pärast mida tellib ta järelauditi.

Kolmeaastase audititsükli jooksul viiakse läbi vähemalt kaks **E-ITS vaheauditi**.

Vaheauditi käigus hindab audiitor:

- põhiauditi käigus tuvastatud lahknevuste käsitlemist;
- infoturbe meetmete rakendusplaani täitmist ning rakendusplaanis tehtud muudatusi;
- organisatsioonis toimunud muudatuste mõju infoturbele;
- organisatsiooni vastupanuvõimet uutele infoturbe ohtudele;
- eelmise E-ITS põhi- või vaheauditi väljajätte;
- E-ITS viimases kehtivas versioonis tehtud muudatuste käsitlemist.

Täiendava vaheauditi tellib auditeeritav, kui on toimunud ISMS käsitusala oluline muutus, mida riigihanke leping ei hõlmanud. Selle käigus hindab audiitor E-ITS nõuete täidetust ja meetmete rakendatust laienenud käsitusalas.

3. E-ITS auditi hankimine

3.1. Riigihanke ese ja riigihanke alusdokumendid

3.1.1. Riigihanke ese

Riigihanke edukaks korraldamiseks tuleb riigihanke alusdokumentides võimalikult täpselt määratleda riigihanke ese.

Auditi puhul on riigihanke esemeks hankija poolt riigihanke alusdokumentides kirjeldatud audiitorteenus.

Audiitorteenuse puhul tuleks hanke eseme kirjeldamisel kindlasti muu hulgas määratleda järgnevad tunnused:

- millist audiitorteenust hangitakse:
 - o vastavusaudit Eesti infoturbe standardi nõuetele,
 - o alternatiivina lubatud EVS-EN ISO 27001:2023 „Infoturbe, küberturbe ja privaatsuskaitse. Infoturbe halduse süsteemid. Nõuded“ sertifitseerimisaudit,
 - o nende standardite nõuetele vastav siseaudit või
 - o audit kokkuleppelise ülesande alusel, mis ei hõlma nimetatud standardite nõudeid ega ole standardile vastavuse siseaudit.
- käsitlusalasse kuuluvate äriprotsesside arv;
- infoturbe halduse süsteemi osised, mida audiitor kontrollib: millised moodulid on rakendatud, milline on käsitlusala, mis ei ole käsitlusalas jne;
- üksus või üksused, milles infoturbe halduse süsteemi rakendatust kontrollitakse. Omaavalitsuse ja selle hallatavate asutuste ühisauditi korral tuleb anda infot ka järgmiste asjaolude kohta:
 - o kas nende infosüsteemid on omavahel seotud,
 - o kas kasutakse ühist infrastruktuuri ja teenuseid;
- andmetöötluse asukohad (kui asukohti on enam kui kolm, ka minimaalne asukohtade arv, milles audit läbi viiakse);
- hankija auditiks valmisoleku aeg;
- audiitorteenuse osutamise muud tingimused, kui hankija soovib neid riigihanke alusdokumentides sätestada.

Arusaadavuse huvides on soovitatav eelpool toodud loetelust vähemalt kolm esimest parameetrit märkida ka riigihanke teates. Täpsemad detailid tuleks esitada riigihanke tehnilises kirjelduses. Näiteks on hankelepingu objektiks „Asutuse A infoturbe halduse süsteemi rakendatuse vastavusaudit/siseaudit Eesti Infoturbe standardi nõuetele vastavuse kohta“.

Juhul, kui hangitakse teenust samaaegselt mitmele asutusele, tuleb see sätestada tehnilises kirjelduses koos viidetega kõigi asutuste äriprotsesside ja asukohtade kohta.

Riigihangete seadus lubab erinevaid teenuseid (näiteks mitme asutuse E-ITS auditeid) koos hankida, seejuures võib ühe riigihanke menetluse raames osadeks jaotada või hankida teenus raamhankena. Hanke osadeks jaotamine või raamhanke kasutamine annaks võimaluse hallata korraga väiksemaid ja jõukohasemaid auditi projekte või kasutada mitmeid teenuspakkujaid nt omaavalitsuse paljude infoturbe vaates sõltumatute hallatavate asutuste auditeerimisel.

Sellise võimaluse kasutamisel on eriti oluline, et hankija toob välja võimalikult täpselt teenuste osade kirjelduse ja viisi, kuidas korraldatakse raamhanke minikonkursid.

Mida rohkem infot on pakkujal hanke objekti kohta, seda lihtsam on täpselt hinnata töö mahtu ning kestust. Täpne arusaamine töö mahust kajastub tõenäoliselt omakorda soodsamas pakkumuse hinnas.

Sageli jääb riigihanke alusdokumentidest arusaamatuks, millist teenust hankija soovib tellida, kuna tehnilises kirjelduses kasutatavad mõisted ei ole arusaadavad. Teenuse liiga üldine või ebatäpne sõnastus võib viia ebaõnnestunud riigihankeni – pakkumisi ei esitata või ületab nende maksumus planeeritu.

Hankedokumentide kirjutamisel tuleks kasutada mõisteid, mis on kasutusel standardite vastavates peatükkides, või Eestis aktsepteeritud Andmekaitse ja infoturbe portaalis (akit.cyber.ee) toodud mõisteid.

Näiteid hangetes esinenud probleemidest

1. Hankija soovis tellida „infoturbe halduse süsteemi auditeerimise nõustamist“. Antud juhul ei ole arusaadav, kas hangitakse „infoturbe halduse süsteemi auditeerimist“ või „infoturbe halduse süsteemi rakendamise nõustamist“ või hoopis koolitust auditiks ettevalmistumiseks. Oluline on selle näite puhul teada, et sertifitseerimis- ja vastavusauditi audiitor erinevalt siseaudiitorist (sõltumatust läbivaatajast) ei tohi nõustada ning enamasti on nõuded audiitorile rangemad. Koos audiitorteenusega ei või ka hankida nõustamisteenust küsimustes, mille kohta hankija soovib audiitorilt hiljem järeldusotsust või aruannet. Vältida tuleb olukorda, kus audiitor vaatab üle iseenda antud konsultatsiooni tulemused või tehtud tööd.
2. Hankija hankis ühe hanke raames nii E-ITS siseauditit kui vastavusauditit. Selline hange võib küll näida mõistlik, kuid tegelikult ei saa neid töid koos hankida. Nimelt on vastavusauditi puhul väga oluline audiitori sõltumatus. Sel põhjusel nõutakse hangetes audiitoritelt ka kinnitust selle kohta, et nad on auditeeritavast asutusest sõltumatud. Siseaudit (E-ITS moodul DER 3.1) või sõltumatu läbivaatus (DER 3.2) seevastu on E-ITS rakendamise üks kohustuslik osa. Lisaks on siseaudit paljuski nõuandva iseloomuga. Seega kontrolliks sellise lepingu puhul audiitor iseenda tööd.
3. Hankija hankis ühe hanke raames ISO 27001 juurutamist ning sertifitseerimisauditit. Ka selline leping sisaldab endas potentsiaalset huvide konflikt. Selline lahendus ei ole ka hankija huvides, kuna tegemist on tarbetu allhankega. Lisaks on sellise töö ajakava määramatu ning igasugune määramatus võib kajastuda kõrgemas hinnas.

3.1.2 Auditi periood

Infoturbe standardid (E-ITS, ISO 27001) näevad tavapäraselt auditite tsükliks ette kolm aastat. Igale täiemahulisele põhiauditile järgnevad aastase vahega kaks vaheauditit. Vajadusel, kui ilmnevad standardite nõuetest olulised lahknevused, lisanduvad järelauditid või käsitusala laienemisel täiendavad vaheauditid.

E-ITS puhul tuleb silmas pidada, et standardi haldaja (RIA) annab igal aastal välja uue versiooni ja selle järgi tuleb ka auditeerida.

Seega tuleks hanke lepingus ja tehnilises kirjelduses ette näha vähemalt kolmeaastane tööde periood põhiauditiks, kuid lepingu kehtivuse aeg peaks olema pikem. EITS lubab samal audiitoril teha audit

samas organisatsioonis kahel järjestikusel perioodil. Kui hankija soovib (aga ei pea) niisugust võimalust kasutada, siis tuleb juhinduda RHS §49 (5)-st ja teha esialgses hanketeates ka sellekohane märge. See märge lihtsustaks oluliselt järgmise hanke korraldamist.

Hanke tehnilises kirjelduses peaks olema märgitud, kui hankijal on selle kohta kindel ootus, millisel ajavahemikul oodatakse audiitorilt toimingute/protseduuride tegemist.

Näiteid hangetes esinenud probleemidest

1. Hankija tellib E-ITS auditi enne, kui auditi eeldused on täidetud. Tulemuseks on auditi venimine ning hiljem vajalikud lepingumuudatused (kuna venima jääb kogu audititsükkel). Audiitor ei tohi ega saa nõustada, seega ei saa loota, et audiitor eelauditi käigus ütleb, kuidas standardit rakendada.
2. Hankija ei ole tegelikult arvestanud oma töötajate olemasolu ja valmisolekuga kokku lepitud (või hankes nõutud) perioodil. Kindlasti ei tohiks auditi tegevusi suvele (juuni-august) ning kohalikes omavalitsustes tasub arvestada ka valimistega.

3.2. Tehniline kirjeldus

Audiitorteenuse kontekstis käsitletakse tehnilise kirjeldusena käesolevas peatükis ja selle alapeatükkides kirjeldatud riigihanke eseme ja audiitorteenuse objekti kohta antavat infot.

Tehnilise kirjelduse koostamisel tuleb kindlasti arvesse võtta seda, et hankija tellib audiitorteenust selleks õigusaktides sätestatud korras, kuid ei saa sätestada piiravaid või suunavaid nõudeid audiitori aruande sisule ja vormile, samuti audiitori töömetoodikale, sest niisugused nõuded võivad mõjutada audiitori sõltumatust. Näiteks ei saa tehnilises kirjelduses ette anda audiitori aruande teatud „omadusi“ (nt, et audiitori aruanne peab olema „märkusteta“ või sisaldama teatud sõnastust) või aruande vormi.

Hankijal ei ole ka ühtegi head põhjust auditi metoodika ettekirjutamiseks (lisaks auditeerimisjuhendis toodule), sest sellelgi võib olla mõju audiitori sõltumatusele.

Hangitava audiitorteenuse kohta tuleb hankijal anda lisaks hanke eseme kirjeldusele vähemalt järgnev info:

- missugune standardi versioon on kasutusel (nt E-ITS puhul ver 2023 või 2024),
- info selle kohta, millal kontrollitava halduse süsteemi osised ja muu audiitorteenuse osutamiseks vajalik teave on hankija poolt audiitorile esitamiseks valmis,
- kas on olemas varasemad auditi (sh ka siseauditi) ja läbivaatuste aruanded,
- info selle kohta, kas hiljuti on olnud olulisi muutusi hankija struktuuris, vara mahus ja koosseisus jms.

Selgituseks. Enamasti on riigihanke objektiks audiitorteenus, mille sisuks on omakorda üks auditeeritav infoturbe halduse süsteem, mille tulemusel väljastatakse üks audiitoraruanne ja järeldusotsus. Kui hangitakse sama audiitorteenust mitme asutuse kohta, siis esitatakse üks audiitori aruanne iga halduse süsteemi kohta.

3.3. Eeldatav maksumus

Auditi eeldatava maksumuse määramine on kahtlemata keeruline ülesanne. Selle töö lihtsustamiseks on siiski mitmeid võimalusi.

Üks levinud võimalus on vaadata Riigihangete registris varasemate edukalt lõppenud hangete infot. Kõigi hangete puhul ei ole kogu info kättesaadav, kuid annab siiski aimu lepingu maksumusest.

Tavapärane on ka, et harvem tellitavate või uute tööde puhul, kui hankija ei tea, missuguseks võib kujuneda teenuse maht, on soovitatav hankijal eelnevalt korraldada turu-uuring (RHS §10) või vajadusel tellida eelnev hinnang või konsultatsioon.

Samuti soovitame juhul, kui hankija ei tea täpselt, mida tal vaja on või milline on soovitava auditi korraldus, küsida esmalt spetsialistidelt nõu. Vastasel korral võib hange venida ning leping ka sõlmimata jääda.

Vältida tasub töömahu alahindamist, kuna sellega tekitatakse oht, et ei esitata ühtki pakkumust, kuna audiitorettevõtted ei soovi teha asjatut tööd.

3.4. Auditi meeskond

RHS näeb ette teenuse pakkuja meeskonna kohta nõuete esitamise kas hindamiseks või pakkuja kvalifitseerimiseks (RHS §85 (8) 2) jagu 3).

Täpsemad nõuded auditi meeskonnale on toodud E-ITS auditeerimisjuhendis.

Asjakohane on esitada kindlad nõuded juhtaudiitorile, kes vastutab ülejäänud meeskonna eest. Auditeerimisjuhend nõuab, et:

- juhtaudiitor on E-ITS auditile eelneva kolme kalendriaasta jooksul osalenud vähemalt kolmes infoturbe halduse süsteemi auditis (sh E-ITS ja ISKE auditid) ning
- tal on vähemalt nelja-aastane IT auditi, IT juhtimise või infoturbe alane töökogemus.

Kui organisatsioonis on kasutusel mõni väga eripärane tehnoloogia, mille puhul on rakendatud väga erilisi infoturvameetmeid, ja on alust arvata, et seetõttu on vajalikud ka eriteadmised auditeerimiseks, siis on asjakohane esitada nõue niisuguste kompetentside olemasoluks auditimeeskonnas.

Ei ole soovitatav esitada piiranguid auditi meeskonna täpsele koosseisule või suurusele. See oleks pakkujale piirav mitmel põhjusel:

- meeskonna liikmetel on erinevad kompetentsid;
- piiratud meeskonna puhul võib olla pärsitud harjumuspärane tööde jaotus meeskonnas, mille tagajärjeks võib olla töö tõhususe kadu;
- kuna auditiprojektid kestavad kolm aastat ning ka hankeprotsess koos lepingu sõlmimisega võib võtta aega, siis vajab ka audiitorfirma paindlikkust oma meeskonna töö korraldamiseks. Paindlikkuse puudumine võib omakorda kajastuda pakkumuse hinnas.

Tasub meeles pidada, et sertifikaatide arv ei näita üheselt inimese kompetentsi ega kogemust ning sertifikaadi ning auditeerimiskogemusega tehniline ekspert võib olla väga vajalik auditi meeskonna liige. Samuti vajavad uued audiitorid kogemust, mida saab vaid auditis osaledes.

3.5. Kõrvaldamise alused

RHS §95 näeb ette pakkujate kõrvaldamise alused, mis loomulikult kehtivad ka infoturbe halduse süsteemi auditi hanke korral.

Vastavalt RHS § 95 lg 4 p 4-le võib hankija kõrvaldada hankemenetlusest pakkuja, kes on raskelt eksinud ametialaste käitumisreeglite vastu. Ainus teadaolev audiitorite kutse-eetika reeglite jälgimist oma ülesandeks võtnu on Eesti Infosüsteemide Audiitorite Ühingu aukohus. Ühingu senise tegevuse vältel ei ole aukohtul tulnud arutada ühtegi eetikakoodeksi rikkumist.

RHS § 95 lg 4 alusel ettevõtja kõrvaldamisel tuleb silmas pidada, et tegemist on hankija kaalutusotsusega, mistõttu tuleb kõrvaldamise otsuses välja tuua põhjused, miks hankija otsustab ettevõtja hankemenetlusest kõrvaldada.

Oluline on arvestada, et infoturbe standardites on tavaliselt sees audiitori sõltumatuse nõue. Ka E-ITS auditeerimisjuhis ütleb, et auditirühma liikmed (juhtaudiitor, teised audiitorid ja kaasatud eksperdid) peavad olema auditeeritavast organisatsioonist sõltumatud ega tohi olla osalenud auditeeritava organisatsiooni infoturbe halduse süsteemi kavandamises või rakendamises, sh organisatsiooni konsulteerimises auditeeritavas valdkonnas, auditi alguskuupäevale eelneva **kolme aasta** jooksul. Auditirühma liikmete sõltumatus peab olema kinnitatud vastava isiku poolt allkirjastatud deklaratsiooniga.

3.6. Kvalifitseerimistingimused

Kvalifitseerimistingimuste koostamisel tuleb silmas pidada, et need oleksid valdkonna tegutsevatele ettevõtjatele arusaadavad ning vajalikud ega oleks põhjendamatult piiravad või koormavad.

Hankijal on kvalifitseerimistingimusena lubatud nõuda:

- kutsealaste oskuste tõendamist. E-ITS nõuded näevad ette CISA või ISO 27001 juhtiva audiitori sertifikaadiga ning vastava kogemusega juhtaudiitori olemasolu audit meeskonnas. Selle tõendamiseks on õigus küsida tõendavat dokumenti, sest neid ei anna välja Eesti organisatsioonid ning andmed ei pruugi olla avalikult kättesaadavad.

- käibe suuruse tõendamist: Vastavalt RHS § 100 lg 1 p-le 4 ning lg-le 3 võib hankija nõuda pakkujal netokäibe olemasolu. Nõuda ei tohi suurema käibe olemasolu kui kahekordne hankelepingu eeldatav maksumus. Näiteks kui hangitakse auditit järgnevas kolmeks aastaks, eeldatav lepingu maksumus kokku kolme aasta kohta on 30 000 eurot ehk 10 000 eurot aastas, on käibenõude arvutuskäik vastavalt $10\,000 \text{ eurot} \times 2 = 20\,000 \text{ eurot}$ majandusaasta kohta ning suurema käibe nõude seadmisel tuleb seda hankijal riigihanke alusdokumentides põhjendada.

- varasema kogemuse tõendamist: RHS § 101 lg 1 p 2 alusel on hankijal lubatud nõuda nimekirja hankija kindlaksmääratud tunnustele vastavate teenuste osutamise lepingutest, mis on täidetud riigihanke algamisele eelneva 36 kuu jooksul, koos teabega nende maksumuse, kuupäevade ja teiste lepingupoolte kohta. Riigihanke alusdokumentide koostamisel peab siinkohal arvestama asjaoluga, et

konfidentsiaalsusnõuetest lähtuvalt võib juhtuda, et audiitorettevõtja ei saa kõigi oma varasemate lepingude detaile avaldada. Lisaks on soovitatav varasemate lepingute mahu nõude seadmisel kaaluda, kas see on proportsionaalne hankelepingu eeldatava maksumuse suhtes (vt ka eelmine punkt).

Lisaks on soovitatav kaaluda, millist infot ja millise detailsusega küsida. Tihti küsitakse lisaks teiste lepingupoolte infole ka lepingu kontaktisiku nime ning kontaktandmeid². Paljude viimase 3 aasta jooksul täidetud lepingute puhul on kontaktisik aga juba asutusest või ettevõttest lahkunud ning tema isikuandmete (mida nimi, meiliaadress ning telefoninumber on) esitamine hankes ei ole korrektne. Lisaks on paljudel juhtudel tegemist riigihangetega ning info lepingu täitmise kohta on riigihangete registrist kättesaadav.

Üldiselt on infoturbe halduse süsteemid oma olemuselt sarnased (NB! Mitte kunagi identsed) ja standardid, mille alusel auditeeritakse, on koostatud nii, et nende nõuded annavad piisava ja tõendatava hinnangu organisatsiooni infoturbe korraldusele ja selle tegelikule olukorrale. Seetõttu täiendavate nõuete esitamine pakkuja kvalifitseerimiseks peab olema väga üksikasjalikult põhjendatud. Erinõuded pädevustele või kogemusele võivad olla vajalikud mõnes tegevusvaldkonnas, millele on seadusandlikult olemas erinõuded (nt usaldusteenustele EL eIDAS määrus, lennuliiklusjuhtimise nõuded, riigisaladuse loa olemasolu vms). Omavalitsustele niisuguste nõuete seadmisi ei ole teada.

Järgnevad kvalifitseerimistingimused võivad tuua kaasa põhjendamatuid riigihankel osalemise piiranguid pakkujatele. Tegu on valiknäidetega varasematel perioodidel koostatud riigihangetest ning aliolev loetelu võimalikest piiravatest tingimustest ei ole ammendav. Selliste tingimuste esitamisel riigihanke alusdokumentatsioonis soovitame, et hankijad kirjutaksid täpsemalt ja selgitavalt lahti, miks need tingimused on seatud ja hankijale vajalikud. Täpsustused ja selgitused aitavad pakkujal hinnata, kas ta ka sisuliselt, mitte ainult vormiliselt, kvalifitseerub.

- rohkem kui üks sertifitseeritud audiitor audiitorettevõttes: kui hankija seab tingimuseks, et audiitorettevõttes peab sertifitseeritud auditoreid olema rohkem kui üks, siis soovitame riigihanke alusdokumentides selgitada, millised on ootused allkirjastava sertifitseeritud audiitori kõrval rohkematele sertifitseeritud audiitoritele, kuna audiitorteenust on võimalik nõuete kohaselt täita, kui auditit juhib ja järeldusotsuse allkirjastab üks sertifitseeritud audiitor, kes esindab audiitorettevõtet.

- eelnev kogemus teatud valdkonnas: omavalitsuste tegevus lähtub õigusaktidest (vt E-ITS profiil kohalikele omavalitsustele <https://www.elvl.ee/eits>), mis kõik on vabalt kättesaadavad kõigile audiitoritele ning sisult puudutavad meie igapäeva elukorraldust. Seetõttu ei ole põhjendatud seada pakkujale piirava tingimusena omavalitsuste auditeerimise kogemust. Küll aga võib seda arvestada hindamisel.

3.7. Hinnatavad näitajad ning pakkumuste hindamine

Pakkumust hinnates võib vastavalt soovile audiitorteenuse hinna kõrval kriteeriumiteks kaaluda näiteks:

- vahetult audiitorteenust teostava(te) audiitori(te) varasem kogemus hangitava audiitorteenuse osutamisel;

² Rangelt võttes peaks pakkuja küsima lepingupartnerilt isikuandmete jagamise nõusolekut. See oleks liigne halduskoormus.

- infoturbe sertifikaati omavate audiitorite arv;
- nii audiitorettevõtte kui konkreetse(te) audiitori(te) varem tehtud auditite arv.

Hindamisel võiks olla hinna ja muude kriteeriumite suhe umbes 70/30.

Punktis 3.6 kirjeldatud kvalifitseerimise tingimusi võib käsitleda ka hinnatavate näitajatenä, kuid NB! üks nõue pakkujale tohib olla kas kvalifitseerimistingimus või hinnatav näitaja.

Soovitav on hindamiskriteeriumite ning –metoodika valik hoolikalt järele mõelda, et see ei eelistaks asjatult mõnd ettevõtet, täidaks eesmärgi (parima pakkumuse valimine) ega oleks pakkujatele asjatult koormav – kui töö maksumus ning pakkumuse esitamiseks vajalik töömaht ei ole vastavuses, siis võib hange läbi kukkuda.

Näiteks on audiitorteenus ning selle sisu E-ITS dokumentides küllalt täpselt kirjeldatud, seega ei ole mõistlik nõuda pakkujalt metoodika ning töö käigu liiga põhjalikku lahti kirjutamist, et seda siis hinnata. See on ajamahukas ega anna ilmselt soovitud tulemust, kuna teenus on ühetaoline ning pakkujate valik piiratud. Lisaks võib pakkuja auditi metoodika sisaldada ärisaladust, mille käsitlemine toob hankijale täiendava halduskoormuse.

Näiteid hangetes esinenud probleemidest

- Asutus küsis E-ITS auditi pakkumusi. Hindamismetoodika nägi ette pakkujate senise kogemuse hindamist. Selleks küsiti pakkujalt seni täidetud E-ITS auditi lepingute andmeid. Paraku ei olnud selleks ajaks ükski nõuetekohane ehk E-ITS auditi leping täidetud, kuna leping sõlmitakse 3 aastaks.
- Asutus küsis samuti ISKE auditi pakkumusi ning hindamismetoodika nägi ette pakkujate senise kogemuse hindamist. Paraku küsiti andmeid viisil (ISKE auditi kogemus aastates, arvestamata, et ühe ISKE auditi aeg oli üsna lühike ning nõutud aja näitamiseks oli vaja pikka ja detailset nimekirja), mis põhjustas pakkujatele väga palju tööd ega toetanud tegelikult tulemuse saavutamist.

Mõlemal korral hankeleping lõpuks sõlmiti, kuid see võttis kavandatust palju rohkem aega.

4. Hankeleping

Hankelepingu projekti koostamisel tuleb jälgida, et hankeleping oleks kooskõlas infoturbe auditeerimise põhimõtetega (nt EVS-EN ISO 19011:2018 Juhtimissüsteemide auditeerimise juhised) ja kutsetegevuse standarditega ning oleks kohustuste ja õiguste poolest osapoolte jaoks tasakaalus.

Lepingus infoturbe halduse süsteemi auditeerimise teenuse tellimiseks peaks osapooltel olema määratud järgnevad komponendid, mis võimaldavad sõlmida hea lepingu ning koostada toimiva auditiplaani:

- a) auditi eesmärgid ja eeldatav ajaline kestus,
- b) auditi käsitusala, sealhulgas auditeeritavad protsessid, organisatsioonilised ja funktsionaalsed üksused sh asukohad,
- c) auditi alusdokumentide iseloomustus ja nende audiitorile edastamise viisid,
- d) hankijapoolne tugi auditi toimingutele,

- e) auditeeritavate asukohtade auditeerimise kuupäevade, eeldatava aja ja kestuse kokkuleppimise viisid,
- f) auditi töö- ja aruandluskeel (erinevus eesti keelest tuleks põhjendada),
- g) eelnevate auditite leiud ja nende alusel sooritatud järeltegevuste kättesaadavus,
- h) ühisauditi korral kooskõlastamine muude auditeerimistoimingutega,
- i) auditi aruande üleandmise viisid,
- j) lepingu sõlmimise, muutmise ja pikendamise tingimused. Nt kui soovitakse jätta võimalus hea koostöö korral sõlmida pakkujaga jätkuleping, tuleks teha lepingus viide RHS §49 lg 5 nõuetele vastavalt. Hankelepingut saab vajadusel muuta RHS §123 tingimustel;

ning vajadusel:

- k) auditirühma liikmete, samuti juhendajate ja vaatlejate rollid ja kohustused,
- l) auditeeritava ja audiitorettevõtte määratud esindaja,
- m) vajadusel logistika- ja sidekorraldus, sealhulgas auditeeritavate asukohtade erikord, konfidentsiaalsuse ja infoturbe seotud küsimused.

Audiitorteenuse hankelepingute sõlmimisel ja nende pikendamisel kohalduvad RHS §120 Hankelepingu sõlmimine ja §123 Hankelepingu muutmine, kuid arvestada tuleks lisaks infoturbe auditi loogikaga.

Käesolevad juhendis käsitletavate infoturbe auditite tavapärane tsükkel on kolm aastat. Otsese nõude sõlmida leping vähemalt 3 aastaks kehtestab E-ITS auditeerimisjuhendi punktis 6.3. Seega on ka auditeerimislepingu kestvus vähemalt kolm aastat, mida saab pikendada veel üheks auditi tsükliks. Viimane piirang tuleb vajadusest säilitada audiitori ja auditeeritava sõltumatus.

Lepingu tähtaega seades tuleb arvestada aga ka sellega, et eelauditi ja põhiauditi vahele võib jääda kuni kuuekuuline periood. Lisaks tuleb kõrgete riskide ilmnemisel tuleb need kõrvaldada ning korraldada järelaudit. Mõlemad pikendavad lepingu täitmise aega.

5. Muude auditite hankimine

Kuigi käesoleva juhendi fookuses on E-ITS auditid, on paljudes organisatsioonides oluline mõista ka teisi levinumaid infoturbe auditi liike. Alljärgnev peatükk annab lühikese ülevaate kolmest olulisest auditist, mida võib olla vaja hankida: ISO 27001 audit, siseaudit (sh E-ITS alusel) ning sõltumatu läbivaatus.

5.1. ISO 27001 audit

Eesmärk

ISO 27001 audit on sertifitseerimisaudit, mille viib läbi akrediteeritud sertifitseerimisasutus eesmärgiga hinnata, kas organisatsiooni infoturbe juhtimissüsteem (ISMS) vastab standardi ISO/IEC 27001 nõuetele.

Kuidas toimub

Audit jaguneb üldjuhul kaheks etapiks:

- Etapp 1 – dokumentatsiooni audit: hinnatakse ISMS-i dokumentatsiooni (sh poliitikad, meetmete kohalduvuse määrang, riskihindamine jms) ja valmidust etapiks 2.

- Etapp 2 – põhjalik audit: hinnatakse ISMS-i rakendamist praktikas. Audiitor viib läbi intervjuud, kogub tõendused nõuete täidetuse ja meetmete rakendatuse kohta, jälgib protsesse.

Sertifikaat kehtib 3 aastat, mille jooksul tehakse iga-aastased järelvalve auditid.

Mida tellides silmas pidada

- Veendu, et organisatsioon on auditiks valmis – nt siseaudit on eelnevalt tehtud, puudused parandatud, tõendusmaterjal nõuete täidetuse ja meetmete rakendatuse kohta olemas.
- Kas audiitorfirma on akrediteeritud.
- Kas audiitoritel on asjakohane kogemus.

Nagu E-ITS auditi puhul, sõlmitakse leping audiitoriga terveks audititsükliks.

5.2. Infoturbe siseaudit (ISO 27001 või E-ITS)

Eesmärk

Siseauditi eesmärk on hinnata organisatsiooni enda poolt seatud infoturbenõuete täitmist. Siseauditit nõuab nii ISO 27001 (peatükk 9.2) kui E-ITS.

Kuidas toimub

- Tavaliselt viib läbi organisatsiooni sisene või väline sõltumatu audiitor.
- Tulemuseks on auditaruanne koos tähelepanekute ja parandusettepanekutega.
- Fookus on sisemisel toimivusel ja pideval parendamisel, mitte formaalsel vastavusel välisele standardile.
- Siseaudiitor ja sõltumatu läbivaataja hindavad ka protsesside tõhusust lisaks toimivusele.

Mida tellides silmas pidada

Kõige olulisem on audiitori valimisel sõltumatus, st audiitor ei tohi olla seotud hinnatava valdkonna igapäevase juhtimise ega meetmete rakendamisega – iseenda tehtud ei saa auditeerida.

Siseaudiitorile täpsemaid nõudeid ei ole, kuid audiitor võiks tunda ISO 27001 või E-ITSi ning omada kogemust (sise)auditeerimisel.

Tihti sõlmitakse siseaudiitoriga leping kogu audititsükliks või ka pikemaks ajaks ning siseauditeid tehakse vastavalt kokku lepitud plaanile (ei pea kõike korraga tegema).

5.3. Sõltumatu läbivaatus

Eesmärk

Vastavalt E-ITSile korraldab organisatsioon regulaarselt infoturbeprotsessi tulemite ja seisundi sõltumatu läbivaatuse. Sõltumatuks läbivaatuseks võib olla ka käsitusala hõlmav siseaudit.

Kuidas toimub

- Sõltumatu läbivaatuse elluvijaks on tavaliselt kas siseaudiitor, väljast tellitud siseaudiitor või käsitusala suhtes asjakohase pädevusega sõltumatu töötaja. Läbivaatusel välditakse kontrollija ja rakendaja rollide huvikonflikti.
- Fookuses võib olla näiteks: riskihindamine, teenusepakkujate haldus vms.
- Tulemuseks on raport või aruanne koos soovitustega.

Mida tellides silmas pidada

- Läbivaatuse tegijaks võib olla ükskõik milline töötaja, kel on selleks vajalikud teadmised ning kes on sõltumatu. Samuti võib läbivaatuse tegijaks olla teise kohaliku omavalitsuse töötaja.
- Veendu, et sõltumatu läbivijaja ei ole seotud hinnatava süsteemi haldusega.

6. Kokkuvõte

Kohalikud omavalitsused seisavad silmitsi ainulaadsete väljakutsete ja vajadustega, kui tegemist on infoturbe tagamise ning auditeerimisega – nõuded on uued, auditi kogemust ei ole ning teadaolevalt on audiitoreid puudu.

Juhend on mõeldud abistama omavalitsusi infoturbe audiitorteenuste hankimisel riigihanke spetsiifikat puudutavates küsimustes, lisades infoturbe halduse süsteemide auditi erijooni. Juhendit koostades on võetud eesmärk aidata hankijatel mõista, kuidas korraldada ja tellida Eesti Infoturbe standardi vastavusaudit, arvestades kohaliku omavalitsuse eripärasid. Juhend sisaldab muuhulgas soovitusi, kuidas saada olukorras, kus auditikohuslaste arv on oluliselt tõusnud ja tõusmas ning audiitorite arv on pea samaks jäänud, soovitud pakkumused ning sõlmida leping, vältides enamlevinud vigu.