

ISKE auditi juhend

Version 1.4

Jaanuar 2017

Sisukord

1. Sissejuhatus	3
2. Mõisted ja lühendid	3
3. ISKE auditi eesmärk.....	3
4. ISKE auditi tellimine.....	3
5. ISKE auditi teostamine.....	4
6. Rakendamisele kuuluvate turvameetmete rakendamise kontroll	4
7. Nõuded ISKE auditi tööde teostajale	5
8. Nõuded ISKE auditi raporti vormistamisele	6
9. Auditi järgsed tegevused	7
10. Versioonid	7

1. Sissejuhatus

Käesolev dokument annab juhiseid ISKE auditite läbiviimiseks. Üldisel tasemel on ISKE auditite läbiviimine reguleeritud Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ (edaspidi nimetatud kui “ISKE määrus”). Käesolevas dokumendis täpsustatakse auditeerimise asjaolusid, mis ei ole määruses sätestatud või mis vajavad täpsustamist ning antakse täiendavaid juhiseid ISKE auditite tellimiseks ja teostamiseks.

2. Mõisted ja lühendid

CISA (*Certified Information Systems Auditor*) - infosüsteemide sertifitseeritud audiitor
infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talituseks vajalike vahendite, ressursside ja protsessidega
ISACA (*Information Systems Audit and Control Association*) – Rahvusvaheline Infosüsteemide Auditi ja Juhtimise Assotsiatsioon
ISKE – infosüsteemide kolmeastmeline etalonturbe süsteem

3. ISKE auditi eesmärk

3.1. ISKE auditi eesmärgiks on hinnata, kas riigi infosüsteemi kuuluva riigi andmekogu(de) pidamisel on ISKE turvameetmed rakendatud.

4. ISKE auditi tellimine

- 4.1. ISKE auditi peavad tellima riigi infosüsteemi kuuluvate riigi andmekogude vastutavad töötlejad sõltuvalt andmekogu turbeastmest vastavalt ISKE määruse §-le 9¹;
 - 4.1.1. Andmekogu vastutav töötleja, kelle andmekogu turbeaste on «H», peab turvameetmete süsteemi rakendamise kohta läbi viima sõltumatu auditi iga kahe aasta järel;
 - 4.1.2. Andmekogu vastutav töötleja, kelle andmekogu turbeaste on «M», peab turvameetmete süsteemi rakendamise kohta läbi viima sõltumatu auditi iga kolme aasta järel;
 - 4.1.3. Andmekogu vastutav töötleja, kelle andmekogu turbeaste on «L», peab turvameetmete süsteemi rakendamise kohta läbi viima sõltumatu auditi iga nelja aasta järel;
- 4.2. ISKE auditi tellib soovitatavalt asutuse siseauditi osakond ja/või siseaudiitor. Kui asutuses puudub siseauditi osakond või siseaudiitor, siis tellib ISKE auditi mõni muu osakond nt. üldosakond.
- 4.3. Kui auditeeritava andmekogu andmeid töödeldakse mitmes erinevas asukohas, peab andmekogu vastutav töötleja määrama hanke kutses või lepingus minimaalse asukohtade arvu, milles audit läbi viiakse. Kui andmeid töödeldakse kolmes või vähemas erinevas asukohas, peab audit katma kõiki asukohti.
- 4.4. Kui asutus tellib ISKE vastavusauditit mitmendat korda, peab ta hanke kutse dokumendis märkima, kas uue auditi moodulite valimi koostamisel arvestatakse eelnevalt auditeeritud moodulid sisse või mitte.

5. ISKE auditi teostamine

- 5.1. Turvameetmete süsteemi rakendamise auditeerimine viiakse läbi infosüsteemi osas, kus andmekogu andmeid töödeldakse.
- 5.2. Auditeerimise käigus tuleb teha muuhulgas järgmised tööd:
 - 5.2.1. kontrollida teostatud infovarade inventuuri vastavust ISKE rakendusjuhendis esitatud nõuetele;
 - 5.2.2. kontrollida turvaklasside ja turbeastmete määramist s.t. kas andmekogule on turvaklassid/turbeaste määratud asjakohaselt;
 - 5.2.3. kontrollida rakendamisele kuuluvate turvameetmete valimist s.t. kas turvameetme valik on tehtud vastavalt ISKE rakendusjuhendis esitatud nõuetest lähtuvalt;
 - 5.2.4. kontrollida kõigi rakendamisele kuuluvate turvameetmete rakendamist (täpsemalt vt. punkt 6);
 - 5.2.5. ISKE auditi võib üheaegselt tellida mitmele andmekogule, sellisel juhul tuleb auditi lõppraportis anda hinnang kõikide andmekogude lõikes.
- 5.3. Punktis 5.2 nimetatud tööde teostamisele eelnevalt tutvub audiitor asutuse infoturbealase dokumentatsiooniga ning hindab, kas asutusel on olemas esmased eeldused ISKE auditi edukaks läbimiseks. Kui dokumentatsiooniga tutvumisel selgub, et auditi edukaks läbimiseks puuduvad vajalikud eeldused, siis soovib audiitor ISKE auditi projektiga mitte jätkata ning anda asutusel võimalus esmased puudused kõrvaldada ning alles seejärel tellida ISKE audit.
- 5.4. ISKE auditi edukaks läbiviimiseks peaksid asutusel olema eelnevalt dokumenteeritud ja teostatud järgmised tööd: ajakohastatud infovarade inventuur, andmekogude kaardistamine ja neile peakasutajate määramine, andmekogudele turvaklasside ja turbeastmete määramine, muudele infovaradele turbeastmete määramine, rakendamisele kuuluvate tüüpmodulite ja turvameetmete loetelude koostamine ja turvameetmete rakendamine. Turvameetmete nimekiri peab olema kirjalikus vormis ning sisaldama minimaalselt ISKE järgseid tüüpmoduleid, rakendamisele kuuluvaid turvameetmeid ja meetme eest vastutajaid, nt kas IT osakond, juhtkond, väline partner volitatud töötaja vms. Juhul, kui asutuses on rohkem kui üks andmekogu, on nimetatud tööd vaja ära teha iga andmekogu lõikes.
- 5.5. Erinevatel aegadel andmekogudele ISKE auditite tellimisel ei pea nn. ühiseid komponente (nt. organisatoorne pool, füüsiline turvalisus) mitmekordselt auditeerima juhul kui eelmisest auditist ei ole möödunud enam aega kui selleks nõutav andmekogude auditeerimise kohustus kehtestab (vt. punkt 4.1).
- 5.6. Audit tuleb üldjuhul läbi viia dokumentatsiooni - ja kohapealse kontrolli abil. Kui kohapealset kontrolli ei ole võimalik teostada, siis võib audiitor tugineda teenuse osutaja dokumentide ja turvasertifikaatide kontrolliga.

6. Rakendamisele kuuluvate turvameetmete rakendamise kontroll

- 6.1. ISKE auditi turvameetme rakendamise kontrolli käigus tuleb kontrollida järgmiste modulite rakendamist:
 - 6.1.1. kõigi B1.0 moodulisse kuuluvate turvameetmete rakendamist;
 - 6.1.2. täiendavalt eelnevale audiitori poolt mooduligruppide B1, B2, B3, B4, B5 valitud rakendamisele kuuluvate modulite ja neis sisalduvate rakendamisele kuuluvate turvameetmete rakendamist. Igast nimetatud mooduligrupist valitakse kaks moodulit. Moodulid valitakse juhusliku valimi meetodit kasutades. Juhusliku valimi koostamise juures peaks viibima tellija esindaja. Kui valiku

- tegemise juures Tellija esindajat ei olnud, tuleb vastav märke teha auditi lõppraportisse. Kokku valitakse sel meetodil täiendavalt kümme moodulit;
- 6.1.3. täiendavalt eelnevale audiitori poolt mooduligruppide B1, B2, B3, B4, B5 valitud rakendamisele kuuluvate moodulite ja neis sisalduvate rakendamisele kuuluvate turvameetmete rakendamist. Igast nimetatud mooduligrupist valitakse kõige kaalukam moodul. Kaalukuse hindamisel võib audiitor arvestada tellija esindaja arvamusega. Kokku valitakse sel meetodil täiendavalt viis moodulit.
 - 6.2. Mitmele andmekogule korraga ja/või mitme asutuse andmekogudele korraga auditi tellimisel ja läbiviimisel tuleb punktis 6.1 kirjeldatud moodulid valida iga auditeerimisele kuuluva andmekogu lõikes eraldi.
 - 6.3. Audiitor võib hinnata täiendavalt muude turvameetmete rakendamist vastavalt vajadusele või teha seda ISKE auditi tellija soovil.
 - 6.4. Kui kohapealset kontrolli ei ole võimalik teostada, siis võib audiitor tugineda teenuse osutaja dokumentide ja turvasertifikaatide kontrolliga.

7. Nõuded ISKE auditi tööde teostajale

- 7.1. Andmekogu vastutav töötleja peab auditeerimise läbiviimisel veenduma, et audiitor omaks auditi läbiviimisel vähemalt ühte järgmistest sertifikaatidest:
 - 7.1.1. Rahvusvahelise Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (*Information Systems Audit and Control Association*) väljaantud infosüsteemide sertifitseeritud audiitori (*Certified Information Systems Auditor, CISA*) sertifikaat. Sertifikaadi kehtivust saab kontrollida veebilehel <https://www.isaca.org/Pages/default.aspx>;
 - 7.1.2. Aktsepteeritakse kõiki ISO 27001 sertifikaati omavaid audiitoreid, kes on leitavad *International Register of Certificated Auditors* veebilehel olevast registrist <http://www.irca.org/home.html>;
 - 7.1.3. Saksa Infoturbeagentuuri (*Bundesamt für Sicherheit in der Informationstechnik*) väljaantud ISO 27001 IT *Grundschutz*i baasil sertifitseeritud audiitori sertifikaat.
- 7.2. Audiitor peab järgima ISKE auditi tegemisel Rahvusvahelise Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (edaspidi ISACA) kutse-eesitika koodeksit, standardeid, suuniseid, protseduurireegleid ja häid praktikaid eesti <http://www.eisay.ee/> ja inglise keeles <http://www.isaca.org>;
- 7.3. ISKE auditi projektis võib osaleda mitu punktis 7.1 nimetatud sertifikaati omavat audiitorit. Sellisel juhul tuleb määrata üks audiitor, kes juhib auditi meeskonna tööd, vastutab auditi käigus teostatavate tööde eest ja kes allkirjastab auditi lõppraporti.
- 7.4. Audiitor peab olema auditeeritavast sõltumatu.
 - 7.4.1. Audiitoriks ei tohi olla isik, kes on auditeerimisele eelnenud kahe aasta jooksul asutust konsulteerinud auditeeritavas valdkonnas.
 - 7.4.2. Audiitori ja iga auditi meeskonda kuuluva asjatundja (kaasa arvatud teiste auditis osalevate audiitorite) sõltumatus peab olema kinnitatud vastavalt audiitori ja auditi meeskonda kuuluva asjatundja poolt allkirjastatud deklaratsiooniga.
- 7.5. Audiitor peab tagama oma kohustuste täitmise käigus omandatud informatsiooni konfidentsiaalsuse.
- 7.6. Audiitor võib ISKE auditis kasutada teiste asjatundjate tööd, järgides seejuures ISACA standardeid.

8. Nõuded ISKE auditi raporti vormistamisele

- 8.1. Auditi lõppraportis annab audiitor hinnangu järgmistele asjaoludele:
 - 8.1.1. kas teostatud infovarade inventuur on viidud läbi vastavalt ISKE rakendusjuhendis esitatud nõuetele, st hinnatakse seoste olemasolu infovarade ja andmekogude vahel, kontrollitakse dokumentatsioonis kajastatud infovarade vastavust tegeliku olukorraga jne;
 - 8.1.2. kas andmekogu(de)le on turvaklassid/turbeaste määratud asjakohaselt, st intervjueeritakse andmekogude omanikke täpsustamaks seadustest, lepingutest, muudest sisemiste protsessidest ning tagajärgede kaalukusest nõudeid andmekogule. Samuti kontrollitakse turvaklassi määramise ja perioodilise ülevaatamise protseduure jne;
 - 8.1.3. kas rakendamisele kuuluvad turvameetmed on valitud korrektselt ja vastavalt ISKE rakendusjuhendis esitatud nõuetele, st kontrollitakse, kas vastavalt infovaradele on meetmete maandamiseks valitud asjakohased ISKE tüüpmodulid ning meetmete valik on õige ning täielik jne;
 - 8.1.4. kas rakendamisele kuuluvad turvameetmed on rakendatud, st rakendamise kontrollimiseks viiakse läbi intervjuusid, uuritakse asutuses loodud dokumentatsiooni ja viiakse läbi testimisi. Iga kontrollitud meetme staatus koos audiitori hinnanguga dokumenteeritakse.
- 8.2. Täiendavalt toob audiitor ISKE auditi lõppraportis välja rakendamata ja/või osaliselt rakendamata turvameetmed, mille mitte rakendamisest ja/või osalisest mitte rakendamisest tulenevad kõrge riskiastmega riskid andmekogu pidamisel.
- 8.3. Iga punktis 8.2 nimetatud turvameetme kohta annab audiitor soovitus ja/või soovitusi, kuidas tuleks nimetatud meetmeid rakendada.
- 8.4. ISKE auditi raportis märgitakse ära kõigi ISKE auditis osalevate audiitorite ja asjatundjate nimed.
- 8.5. ISKE auditi lõppraporti lissasse tuleb panna kõigi auditeeritud turvameetmete tabel, milles on audiitori poolt muuhulgas iga turvameetme järgi märgitud, kas turvameede on rakendatud, on osaliselt rakendatud, ei ole rakendatud, ei saa rakendada, ei rakendata.
- 8.6. Juhul kui vastutav töötleja on otsustanud mõnda turvameedet mitte rakendada s.t. eelmises punktis nimetatud staatus "ei rakenda", siis audiitor hindab selle turvameetme mitterakendamise põhjenduse piisavust ning selle mitterakendamisest tulenevaid riske ja annab seejärel oma hinnangu, kas turvameetme mitterakendamine on põhjendatud.
- 8.7. Iga osaliselt rakendatud turvameetme järgi kirjutab audiitor puuduse(d), mis osas on turvameede rakendamata ja esitab soovitus(ed) puudus(t)e likvideerimiseks.
- 8.8. ISKE auditi lõppraporti lissadesse tuleb panna auditi meeskonna poolt ISKE auditi käigus loodavad muud dokumendid ja iga tähelepaneku ning soovitus(e) korral tuleb viidata asitõenditele millele soovitus või tähelepanek tugineb nt. testimiste ja vaatluste tulemused, intervjuud, läbitöötatud juhendid ja protseduurireeglid jmt, mille alusel audiitor hinnangu andis.
- 8.9. ISKE auditi lõppraport tuleb vormistada selliselt, et auditeeritaval oleks võimalik osaliselt rakendamata ja rakendamata meetmete järele tekitada lisaveerud, kuhu saab kanda meetme rakendamise eest vastutaja ja tähtaja.

9. Auditi järgsed tegevused

- 9.1. Vastutav töötleja on kohustatud võimalikult kiiresti rakendama auditi lõppraportis märgitud kõrge riskiastmega meetmed ja ülejäänud rakendamata meetmed rakendama mõistliku aja jooksul.
- 9.2. Kõrge riskiastmega meetmete rakendamise kohta tuleb tellida koheselt peale nende rakendamist järelaudit, mille võib läbi viia audiitor, kes vastab punktis 7.1 toodud nõuetele. Järelauditi võib teostada sama audiitor, kes esialgse auditi läbi viis.
- 9.3. Järelauditi käigus auditeeritakse ainult nende turvameetmete rakendamist, mille kohta tehti kõrge riskiastmega märkus(i).
- 9.4. Ühe kuu jooksul pärast auditi teostamist märgib andmekogu vastutav töötleja riigi infosüsteemi halduse infosüsteemi ISKE auditi tulemuse.

10. Versioonid

Versioon redigeerija kuupäev kommentaar

1. 0 Toomas Viira 8.1.10 esmatrükk

1. 1 Toomas Viira 11.8.10 Lisati punkt 6.2

1. 2 Aare Reintam 13.7.11 Muudeti punkte 5.2.5; 5.4; 6.1.2; 6.1.3;
7.1.2; 7.2; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.7; 8.8

ja lisati punktid ; 7.7 ja 8.9

1.3 Aare Reintam 8.12.2011 Muudeti punkti 9.2 ja lisati punkt 7.8

1.4 Jana Roosimägi, Elsa Neeme 17.10.2016, tõsteti punktid 7.7 ja 7.8 punkti 4 alla, täiendati punktidega 5.6, 6.4.