Riigi Infosüsteemide Arenduskeskus

# ISKE auditi juhend

Versioon 1.1

August 2010

## Sisukord

## 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 § $9^1$ (1) – (3);

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 soovitavalt asutuse siseauditi osakond ja/või siseaudiitor. Kui asutuses puudub siseauditi osakond või siseaudiitor, siis tellib ISKE auditi mõni muu osakond nt. üldosakond.

## 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;

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 soovitab audiitor ISKE auditi projektiga mitte jätkata ning anda asutusel võimalus esmased puudused kõrvaldada ning alles seejärel tellida ISKE audit;

5.4. ISKE edukaks läbiviimiseks peaksid asutusel olema eelnevalt dokumenteeritud ja teostatud vähemalt järgmised tööd: infovarade inventuur, andmekogude kaardistamine ja neile peakasutajate määramine, andmekogudele turvaklasside ja turbeastmete määramine, muudele infovaradele turbeastmete määramine, rakendamisele kuuluvate tüüpmoodulite ja turvameetmete loetelude koostamine ja turvameetmete rakendamine;

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).

## 6. Rakendamisele kuuluvate turvameetmete rakendamise kontroll

6.1. Andmekogu ISKE auditi turvameetme rakendamise kontrolli käigus tuleb kontrollida järgmiste moodulite rakendamist:

6.1.1. Kõigi B1.0 moodulisse kuuluvate turvameetmete rakendamist;

6.1.2. Täiendavalt eelnevale audiitori poolt mooduligruppidest B1, B2, B3, B4, B5 valitud rakendamisele kuuluvate moodulite ja neis sisalduvate rakendamisele kuuluvate turvameetmete rakendamist. Igast nimetatud mooduligrupist valitakse kaks moodulit. Moodulid valitakse juhusliku valimi meetodit kasutades. Kokku valitakse sel meetodil täiendavalt kümme moodulit;

6.1.3. Täiendavalt eelnevale audiitori poolt mooduligruppidest B1, B2, B3, B4, B5 valitud rakendamisele kuuluvate moodulite ja neis sisalduvate rakendamisele kuuluvate turvameetmete rakendamist. Igast nimetatud mooduligrupist valitakse üks moodul. Moodulid valitakse lähtudes mooduli kaalukuse hinnangust. 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 ISKE auditi tellija soovil.

## 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;

7.1.2. Briti Standardi Instituudi (*British Standards Institute*) väljaantud ISO 27001 juhtiva audiitori sertifikaat;

7.1.3. Saksa Infoturbeagentuuri (*Bundesamt für Sicherheit in der Informationstechnik*) väljaantud ISO 27001 IT *Grundschutzi* baasil sertifitseeritud audiitori sertifikaat;

7.2. Audiitor peab järgima ISKE auditi tegemisel Rahvusvahelise Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (edaspidi ISACA) kutse-eetika koodeksit, standardeid, suuniseid, protseduurireegleid ja häid (eesti keeles http://www.eisay.ee/vvfiles/2/ISACA_standardid_suunised_protseduurid.pdf ja inglise keeles http://www.isaca.org/AMTemplate.cfm?Section=Standards2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=52295);

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 säilitama 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;

8.1.2. kas andmekogu(de)le on turvaklassid/turbeaste määratud asjakohaselt;

8.1.3. kas rakendamisele kuuluvad turvameetmed on valitud korrektselt ja vastavalt ISKE rakendusjuhendis esitatud nõuetele;

8.1.4. kas rakendamisele kuuluvad turvameetmed on rakendatud;

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 soovituse 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 lisasse 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;

8.8. ISKE auditi lõppraporti lisadesse tuleb panna auditi meeskonna poolt ISKE auditi käigus loodavad muud dokumendid ja/või kogutud asitõendid nt. testimiste tulemused, vaatluste tulemused jmt.

## 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;

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.