Väljaandja:	Teede- ja Sideminister
Akti liik:	määrus
Teksti liik:	algtekst-terviktekst
Redaktsiooni jõustumise kp:	01.06.2002
Redaktsiooni kehtivuse lõpp:	31.08.2014
Avaldamismärge:	RTL 2000, 108, 1655

Teenuse osutajate infosüsteemide auditeerimise kord

Vastu võetud 03.10.2000 nr 83

Määrus kehtestatakse «Digitaalallkirja seaduse» (RT I 2000, 26, 150) paragrahvi 43 lõike 4 alusel.

1. peatükk
ÜLDSÄTTED

§ 1. Käesolev määrus reguleerib teenuse osutaja infosüsteemi auditeerimist, eesmärgiga määrata kindlaks infosüsteemi kasutuskõlblikkus ning vastavus õigusaktidega kehtestatud nõuetele ja normidele.

§ 2. Audit viiakse läbi:
1) teenuse osutaja kandmiseks sertifitseerimise riiklikku registrisse;
2) igal aastal teenuse osutaja sertifitseerimise riiklikku registrisse kandmise kuupäevaks.

§ 3. Auditi tellib audiitorilt teenuse osutaja (edaspidi *TO*).

2. peatükk
AUDIITOR

§ 4. Audiitoriks võib olla füüsiline isik, kes omab auditi läbiviimise ajal kehtivat rahvusvahelist Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (*Information Systems Audit and Control Association*) poolt väljaantud infosüsteemide sertifitseeritud audiitori (*Certified Information Systems Auditor, CISA*) sertifikaati.

§ 5. Audiitor peab olema sõltumatu teenuse osutajast, keda ta auditeerib. Audiitori sõltumatus peab olema kinnitatud allkirjastatud dokumendiga.

§ 6. Audiitor on kohustatud säilitama oma kohustuste täitmise käigus omandatud informatsiooni konfidentsiaalsust.

3. peatükk
AUDITI LÄBIVIIMINE

§ 7. Auditeerimine viiakse läbi TO infosüsteemi osas, mis on vajalik vastava teenuse osutamiseks.

§ 8. Sertifitseerimisteenuse osutaja esitab auditi läbiviimiseks dokumenteeritud sertifitseerimispõhimõtted vastavalt seadusele.

§ 9. Ajatempliteenuse osutaja esitab auditi läbiviimiseks dokumenteeritud ajatembelduspõhimõtted vastavalt seadusele.

§ 10. Auditi läbiviimiseks esitatakse materjalid ja dokumendid, mis tõendavad TO kohustuste täitmist vastavalt «Digitaalallkirja seadusele» ning teenuse osutaja infosüsteemi konfiguratsiooni halduse dokumentatsiooni.

§ 11. Kui TO on pärast eelmise auditi toimumist teinud käesoleva määruse paragrahvides 9–11 märgitud dokumentides muudatusi, on ta kohustatud esitama kõik nendest dokumentidest kinnitatud versioonid koos nende kehtimise ajavahemikega.

§ 12. TO on kohustatud esitama audiitori nõudmisel täiendavaid dokumente ja andmeid, mis on vajalikud auditi läbiviimiseks.

§ 13. Auditi teostamisel peab TO tagama audiitorile juurdepääsu oma infosüsteemile.

§ 14. Auditi käigus teostatakse normidele ja nõuetele vastavuse kontroll audiitori määratud kontrollsisendites ja -väljundites.

§ 15. Auditi käigus kontrollitakse:
1) kas TO on rakendanud asjakohast professionaalset hoolikust kvaliteetse ja turvalise teenuse tagamiseks;
2) TO infosüsteemi vastavust «Digitaalallkirja seadusele», «Isikuandmete kaitse seadusele», «Andmekogude seadusele» ja teiste õigusaktidega kehtestatud ning käesoleva määruse paragrahvi 16 nõuetele;
3) mittevastavusi käesoleva paragrahvi punktis 2 esitatud nõuetele tuleb põhjendada auditi raportis;
4) TO infosüsteemi, sealhulgas organisatsiooni ja töökorralduse vastavust dokumenteeritud sertifitseerimispõhimõtetele;
5) ajatempliteenuse osutaja infosüsteemi, sealhulgas organisatsiooni ja töökorralduse vastavust dokumenteeritud ajatembelduspõhimõtetele;
6) teenuse osutaja kohustuste täidetust vastavalt «Digitaalallkirja seadusele»;
7) teenuse osutaja infosüsteemi vastavust standardile EVS-ISO/IEC 12207, märkides aruandes, millistele standardi osadele vastavust kontrolliti;
8) teenuse osutaja infosüsteemi turbe vastavust standarditele EVS-ISO/IEC TR 13335-1,2,3 ja ISO/TR 13569, märkides aruandes, millistele standardi osadele vastavust kontrolliti;
9) TO infosüsteemi vastavust materjalile «COBIT (*Control Objectives for Information and Related Technology*) Auditi suunised, aprill 1998, 2. redaktsioon. Infosüsteemide auditi ja juhtimise fondi väljaanne.» Aruandes märgitakse, millistele osadele vastavust kontrolliti;
10) TO infosüsteemi vastavust spetsiifilistele sertifitseerimis- või ajatempliteenuse osutamisega seotud nõuetele; aruandes märkida, millistele nõuetele vastavust kontrolliti;
11) TO infosüsteemi vastavust muudele teenuse osutamise seisukohast olulistele õigusaktidega kehtestatud tehnilistele normidele ja nõuetele.

§ 16.TO-le esitatavad täpsustatud nõuded:
1) sertifikaadi omaniku identifitseerimine on usaldusväärne;
2) sertifikaadi omanikult nõutakse vaid informatsiooni, mis on vajalik antud teenuse kvaliteetseks osutamiseks;
3) väljaantud sertifikaatides on näidatud sertifikaadi taotleja poolt esitatud kasutusvaldkonna piirangud;
4) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagab teenuse osutaja juures hoitava avaldamisele mittekuuluva teabe saladuses hoidmise kolmandate isikute eest;
5) sertifikaatide omanike poolt esitatavate avalduste ja teiste dokumentide säilitamine ja arhiveerimine on korraldatud kvaliteetselt ja turvaliselt;
6) teenuse osutaja auditeeritavat infosüsteemi kasutatakse vaid selleks ette nähtud otstarbeks, süsteemis on realiseeritud funktsioonid, mis teenuse osutamise põhimõtetes on kirja pandud, kogu kasutatav tarkvara on usaldusväärne ja seaduslik;
7) süsteemis toimuvaid teenuse osutamisega seotud tegevusi on tagantjärele võimalik kontrollida;
8) on korraldatud efektiivne kaitse infotehnoloogiliste rünnete vastu;
9) on garanteeritud sertifitseerimis- või ajatempliteenuse jätkuvus ja kasutajate huvide kaitse juhul, kui sertifikaatide väljaandmisel kasutatavat sertifitseerimisteenuse osutaja esindaja isiklikku võtit on võimalik kasutada tema nõusolekuta;
10) eksisteerivad turvalised ja efektiivsed protseduurid teenuse osutaja avaliku võtme avalikustamiseks, sertifikaatide säilitamiseks ning vajadusel nende üleandmiseks mõnele teisele teenuse osutajale;
11) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega ning väljaantud sertifikaatide, tõendite ja nende üldkasutatavas andmesidevõrgus edastamise mehhanismidega võimaldavad üldkasutatava andmesidevõrgu vahendusel efektiivselt ja ööpäevaringselt kontrollida sertifikaadi kehtivust käesoleval või mingil varasemal ajahetkel;
12) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega välistavad teenuse osutaja teeskluse üldkasutatavas andmesidevõrgus kõikides sertifikaadiga seotud toimingutes, sealhulgas sertifikaadi väljaandmisel, kontrollimisel, peatamisel ja kehtetuks tunnistamisel;
13) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagavad selle, et teenuse osutaja ei saa tühistatud või peatatud sertifikaadi kohta väita selle kehtivust ning vastupidi – kehtiva sertifikaadi korral on välistatud teenuse osutaja väide selle tühistamise või peatamise kohta;
14) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagavad sertifikaatide kehtivuse peatamise või sertifikaadi kehtetuks tunnistamise avalduste vastuvõtmise ööpäevaringselt üldkasutatavate andmesidevõrkude vahendusel;
15) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagavad kohe sertifikaadi kehtivuse peatamise või sertifikaadi kehtetuks tunnistamise pärast vastava volitatud avalduse saabumist;
16) sertifitseerimisteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega välistavad sertifikaadi kehtivuse peatamise või sertifikaadi kehtetuks tunnistamise volitamatute avalduste aktsepteerimise.
17) ajatempliteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagavad, et ajatempleid saab ööpäevaringselt võtta ning kontrollida üldkasutatava andmesidevõrgu vahendusel;
18) ajatempliteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagavad selle, et kahte teenuse osutaja poolt välja antud ajatemplit on hiljem alati võimalik võrrelda, tehes sellega kindlaks nende andmise ajalise järgnevuse;
19) ajatempliteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega tagavad, et on välistatud ajatemplite võtmine taotletavast ajahetkest hilisemale või varasemale ajale;
20) ajatempliteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega välistavad võltsajatemplite aktsepteerimise;
21) ajatempliteenuse osutaja infosüsteem koos organisatsiooniliste vahenditega välistavad ajatempli teenuse osutaja teeskluse teenuse osutamisel.

§ 17.Käesoleva määruse paragrahvis 15 nimetatud kontrolltoimingute kohta vormistatakse protokollid.

4. peatükk

AUDITI TULEMUSED

§ 18. Audit loetakse läbituks, kui auditi tulemusena TO infosüsteem vastab kehtestatud nõuetele.

§ 19. Auditi koondtulemused esitatakse teenuse osutajale auditi raportis, millele audiitor on andnud oma allkirja. Raportis esitatakse muu hulgas:
1) teenuse osutaja kinnitus auditi toimumise kohta antud ajavahemikul;
2) audiitori andmed, sealhulgas kinnitus kehtiva CISA sertifikaadi omamise kohta;
3) auditi teostamise ajavahemik;
4) auditi teostamise käik, leiud, hinnangud ja järeldused vastavalt käesoleva määruse paragrahvis 15 sätestatud nõuetele;
5) audiitori otsus TO infosüsteemi vastavuse kohta käesolevas määruses esitatud nõuetele.

§ 20. Raportile lisatakse vajadusel detailsed aruanded.

§ 21. Audiitor säilitab auditi raportit ja muid sellega seonduvaid dokumente vähemalt kolme aasta jooksul pärast auditi toimumist.

§ 22. Audiitor peab nõudmisel esitama täiendavaid andmeid auditi tulemuste kontrollijale.

Minister Toivo JÜRGENSON
Kantsler Margus LEIVO