AS Sertifitseerimiskeskus

Sertifitseerimisteenuse ja ajatempliteenuse osutaja infosüsteemi auditi raport

KPMG Estonia
8. oktoober 2004
Dokument koosneb 6 leheküljest
SK 041007 raport.rtf

Sisukord

1 Kokkuvõte

1.1 Auditi eesmärk

Meie eesmärgiks oli läbi viia AS-i Sertifitseerimiskeskus infosüsteemide audit vastavalt Teede- ja sideministri 3. oktoobri 2000. a. määrusele nr. 83 "Teenuse osutajate infosüsteemide auditeerimise kord". Määrus reguleerib sertifitseerimis- ja ajatempliteenuse osutaja infosüsteemi auditeerimist, eesmärgiga määrata kindlaks infosüsteemi kasutuskõlblikkus ning vastavus õigusaktidega kehtestatud nõuetele ja normidele.

1.2 Audiitorite andmed

Auditi viis läbi KPMG Estonia töötaja Jüri Tirmaste, infosüsteemide audiitor (CISA sertifikaadi andmed – vt. Lisa 2);

1.3 Auditi teostus

Viisime auditi läbi ajavahemikus 7. septembrist kuni 6. oktoobrini 2004. a. Tööde käigus tutvusime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna ja dokumentatsiooniga, intervjueerisime võtmeisikuid, jälgisime tööprotsesse ning viisime läbi muid kontrolli-protseduure.

1.4 Audiitori otsus

Oleme auditeerinud AS-i Sertifitseerimiskeskus infotehnoloogilist keskkonda. Arvame, et meie audit annab piisava aluse arvamuse avaldamiseks AS-i Sertifitseerimiskeskus infosüsteemi kohta.

Oleme seisukohal, et AS-i Sertifitseerimiskeskus infosüsteem vastab Teede- ja sideministri 3. oktoobri 2000. a. määruses nr. 83 "Teenuse osutajate infosüsteemide auditeerimise kord" esitatud nõuetele.

2 Hinnangud ja järeldused

Käesoleva raportiosa "Hinnangud ja järeldused" ülesehitus järgib Teede- ja sideministri 3. oktoobri 2000 määrusega nr. 83 kinnitatud "Teenuse osutajate infosüsteemide auditeerimise korra" §15 struktuuri. Määrust on tsiteeritud ***kursiivis ja rasvaselt***.

2.1 Kvaliteetne ja turvaline teenus

Kontrollitakse, kas TO on rakendanud asjakohast professionaalset hoolikust kvaliteetse ja turvalise teenuse tagamiseks.

Arvestades AS-i Sertifitseerimiskeskus personalipoliitikat, töötajate kvalifikatsiooni, põhjalikkust ja konservatiivsust kriitilistes valdkondades, väljakujunenud töömeetodeid ning olemasolevat infotehnoloogilist keskkonda oleme arvamusel, et ettevõte on võimeline jätkuvalt tagama sertifitseerimisteenuse ja ajatempliteenuse kvaliteeti ja turvalisust.

2.2 Vastavus õigusaktidele

Kontrollitakse TO infosüsteemi vastavust «Digitaalallkirja seadusele», «Isikuandmete kaitse seadusele», «Andmekogude seadusele» ja teiste õigusaktidega kehtestatud ning käesoleva määruse paragrahvi 16 nõuetele.

Olemasolev infotehnoloogiline keskkond ja selle plaanitavad arendused ei sea takistusi infosüsteemi vastavuse tagamisel kehtivatele õigusaktidele. AS-i Sertifitseerimiskeskus infosüsteem vastab määruse paragrahvis 16 esitatud täpsustatud nõuetele.

2.3 Põhjendused mittevastavustele

Mittevastavusi käesoleva paragrahvi punktis 2 [käesoleva raporti punktis 2.2] ***esitatud nõuetele tuleb põhjendada auditi raportis.***

Nimetatud mittevastavusi auditi käigus ei avastatud.

2.4 Vastavus sertifitseerimispõhimõtetele

Kontrollitakse TO infosüsteemi, sealhulgas organisatsiooni ja töökorralduse vastavust dokumenteeritud sertifitseerimispõhimõtetele.

Ettevõtte infosüsteem, organisatsioon ja töökorraldus vastavad dokumenteeritud sertifitseerimispõhimõtetele.

2.5 Vastavus ajatembelduspõhimõtetele

Kontrollitakse ajatempliteenuse osutaja infosüsteemi, sealhulgas organisatsiooni ja töökorralduse vastavust dokumenteeritud ajatembelduspõhimõtetele.

Ettevõtte infosüsteem, organisatsioon ja töökorraldus vastavad dokumenteeritud ajatembelduspõhimõtetele.

2.6 DAS kohustuste täidetus

Kontrollitakse teenuse osutaja kohustuste täidetust vastavalt «Digitaalallkirja seadusele».

Kinnitame, et AS Sertifitseerimiskeskus vastab Digitaalallkirja seaduse §18 lõige (1) punktis 1, §25 punktis 1, §19 ja §26 esitatud kriteeriumitele ning on võimeline täitma §22 loetletud sertifitseerimisteenuse osutaja ja §28 loetletud ajatempliteenuse osutaja kohustusi.

2.7 EVS-ISO/IEC 12207

Kontrollitakse teenuse osutaja infosüsteemi vastavust standardile EVS-ISO/IEC 12207, märkides aruandes, millistele standardi osadele vastavust kontrolliti.

Kontrollisime vastavust standardi EVS-ISO/IEC 12207 osale 5.3 “Arendusprotsess”, keskendudes rakendustarkvara arendusele. Meie hinnangul vastab nimetatud protsess standardile.

2.8 EVS-ISO/IEC TR 13335

Kontrollitakse 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.

Kontrollisime ettevõtte infoturbekorralduse vastavust standardi EVS ISO/IEC TR 13335-3 “Infoturbe halduse suunised. Osa 3: Infoturbe halduse meetodid” peatükile 7 “Infoturbe eesmärgid, strateegia ja poliitikad”. Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib infoturbe korraldamisel jätkuvalt standardis esitatud põhimõtteid.

Kontrollisime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna vastavust standardi ISO/TR 13569 peatüki 7 “Turvameetmete teostus” osale 7.7 “Tarkvara”. Oleme arvamusel, et AS Sertifitseerimiskeskus on järginud standardis esitatud nõudeid.

2.9 COBIT

Kontrollitakse 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.

Kontrollisime vastavust COBIT-i protsessidele DS11 "Hallata andmeid" ja DS13 "Hallata ekspluatatsiooni". Meie hinnangul on AS Sertifitseerimiskeskus järginud standardi nõudeid.

2.10 Spetsiifilised nõuded

Kontrollitakse TO infosüsteemi vastavust spetsiifilistele sertifitseerimis- või ajatempliteenuse osutamisega seotud nõuetele; aruandes märkida, millistele nõuetele vastavust kontrolliti.

Kontrollisime vastavust standardi ETSI TS 101 456 "*Policy requirements for certification authorities issuing qualified certificates*" osa 6 "*Obligations and liability*" ja osa 7 "*Requirements on CA practice*" ning standardi ETSI TS 102 023 "*Policy requirements for time-stamping authorities*" osa 7 "*Requirements on TSA practices*" nõuetele.

Jõudsime seisukohale, et AS Sertifitseerimiskeskus on järginud nimetatud standardites esitatud head tava vastavalt ettevõtte suurusest tulenevale otstarbekusele, järgides eelkõige Eestis kehtivaid õigusakte.

2.11 Muud tehnilised normid

Kontrollitakse TO infosüsteemi vastavust muudele teenuse osutamise seisukohast olulistele õigusaktidega kehtestatud tehnilistele normidele ja nõuetele.

Auditi läbiviimise ajaks ei olnud õigusaktidega kehtestatud muid teenuse osutamise seisukohast olulisi tehnilisi norme ja nõudeid.

Tallinnas, 8. oktoobril 2004. a.

Lugupidamisega

(allkirjastatud digitaalselt)

Jüri Tirmaste
infosüsteemide audiitor, CISA

Lisad:
1. Kinnitus auditi toimumise kohta antud ajavahemikul
2. Kinnitus audiitori sõltumatuse ja CISA sertifikaadi omamise kohta