AS Sertifitseerimiskeskus

Sertifitseerimisteenuse ja ajatempliteenuse osutaja infosüsteemi auditi raport

KPMG Estonia
7. oktoober 2002
Dokument koosneb 9 leheküljest
SK 021007 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 viisid läbi järgmised KPMG Estonia töötajad:

- Jüri Tirmaste, infosüsteemide audiitor (CISA sertifikaadi andmed – vt. Lisa 2);
- Erik Tambaur, konsultant.

1.3 Auditi teostus

Viisime auditi läbi ajavahemikus 10. septembrist kuni 7. oktoobrini 2002. a. Tööde käigus tutvusime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna ja dokumentatsiooniga, intervjueerisime võtmeisikuid, jälgisime tööprotsesse ning viisime läbi muid kontrolliprotseduure.

1.4 Auditi tulemust mõjutavad asjaolud

AS Sertifitseerimiskeskus soovib alustada ajatempliteenuse pakkumist. Johtuvalt asjaolust, et infosüsteemi auditi läbiviimine on ajatempliteenuse osutamise eeltingimuseks, ei olnud meil võimalik tutvuda tööprotsessidega, mis käivituvad alles teenuse osutamisel. Seega polnud meil võimalik täielikult kontrollida töökorralduse vastavust AS-i Sertifitseerimiskeskus ajatembelduspõhimõtetele.

1.5 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.

AS-i Sertifitseerimiskeskus töötajate hinnangul saavutab ettevõte valmisoleku ajatempliteenuse pakkumiseks oktoobris 2002, mis on meie arvamuse kohaselt reaalne.

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 kinnitame, et ettevõte on võimeline jätkuvalt tagama kavandatava teenuse 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 sertifitseerimisteenust puudutavas osas. Olemasolev infotehnoloogiline keskkond ja selle plaanitavad arendused ei sea takistusi infosüsteemi vastavuse tagamisel määruse ajatempliteenuse osutamisega seotud 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 selgunud.

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 infosüsteemi arhitektuur, selle komponendid ja lähiajal kavandatud arendused vastavad üldjoontes olemasolevatele ajatembelduspõhimõtetele. Töökorralduse vastavust ajatembelduspõhimõtetele ei ole enne teenuse osutamise alustamist võimalik hinnata.

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 5.4 “Ekspluatatsiooniprotsess”, keskendudes ID-kaardiga seotud toiminguid registreeriva rakenduse Pedaal ekspluatatsioonile ja kasutajatoele. 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 10 “Infoturbeplaani täitmine”. Jõudsime järeldusele, et AS Sertifitseerimiskeskus on infoturbe korraldamisel järginud standardis esitatud põhimõtteid. Leidsime lahknevusi standardi kitsalt spetsifitseeritud nõuete osas, mille täitmine väikesearvulise töötajaskonnaga ettevõttes ei olekski põhjendatud.

Kontrollisime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna vastavust standardi ISO/TR 13569 peatüki 7 “Turvameetmete teostus” osadele 7.2 “Loogilise pääsu reguleerimine” ja 7.6 “Võrgud”. Oleme arvamusel, et AS Sertifitseerimiskeskus on järginud nimetatud 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 DS3 "Hallata suutlikkust ja võimsust" ning DS4 "Tagada pidev teenus". Lahknevused standardist ilmnesid juhtimiseesmärgis DS 3.4 "Modelleerimisvahendid". Meie arvates on ilmnenud lahknevused antud suurusega infotehnoloogilise keskkonna kontekstis ebaolulised ja ei takista DS3 ärinõuete täitmist.

DS4 osas on lahknevuseks mõnede ajatempliteenuse osutamisega seotud infosüsteemi komponentide taasteplaani puudumine. Kavas on vastavad plaanid koostada arendustööde lõppemisel ja olukorra stabiliseerumisel. Lahknevus ilmnes juhtimiseesmärgis DS 4.11 "Varuasukoht ja -riistvara" – nimetatud ressursse ei ole veel soetatud, sest serveriruumi ja kõikide seadmete dubleerimine on äärmiselt kulukas.

Arvestades serveriruumi füüsilise turvalisuse head taset võime siiski kinnitada, et AS Sertifitseerimiskeskus on olemasolevate võimaluste piires teinud endast sõltuva pideva teenuse tagamiseks.

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 7.4 "*CA management and operation*" ning standardi ETSI TS 102 023 "*Policy requirements for time-stamping authorities*" osa 7 "*Requirements on TSA practices*" nõuetele. Kontrolli tulemusena täpsustatakse ajatembelduspõhimõtteid mõnede ETSI TS 102 023 standardist tulenevate spetsiifiliste nõuete osas.

Jõudsime seisukohale, et AS Sertifitseerimiskeskus on järginud nimetatud standardites esitatud head tava vastavalt osutatavate teenuste iseloomule ja ettevõtte suurusest tulenevale otstarbekusele.

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.

Lugupidamisega

Jüri Tirmaste
infosüsteemide audiitor, CISA

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

Koopiad: 2 (kaks) koopiat AS-le Sertifitseerimiskeskus, neist 1 (üks) esitamiseks Sertifitseerimise riiklikule registrile

Lisad

Lisa 1. Kinnitus auditi toimumise kohta antud ajavahemikul

Vastavalt Teede ja sideministri 3. oktoobri 2000 määruse nr. 83 §19 punktile 1 kinnitab AS Sertifitseerimiskeskus, et käesoleva raporti aluseks olnud infosüsteemi audit viidi läbi KPMG Estonia infosüsteemi audiitori Jüri Tirmaste poolt ajavahemikus 10. septembrist kuni 7. oktoobrini 2002. a.

Tallinnas, 7. oktoobril 2002. a.

Ain Järv
juhataja
AS Sertifitseerimiskeskus

Lisa 2. Kinnitus audiitori sõltumatuse ja CISA sertifikaadi omamise kohta

Oleme tutvunud Teede ja sideministri 3. oktoobri 2000 määrusega nr. 83 kinnitatud Teenuse osutajate infosüsteemide auditeerimise korraga (Kord) ning kinnitame, et AS-i Sertifitseerimiskeskus infosüsteemi auditeerimisel vastab KPMG Estonia infosüsteemide audiitor Jüri Tirmaste Korra §-s 5 esitatud audiitori sõltumatuse nõudele.

Samuti kinnitame, et Jüri Tirmaste omas auditi läbiviimise ajal kehtivat infosüsteemide sertifitseeritud audiitori CISA sertifikaati nr. 0227942, mis on välja antud Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (*Information Systems Audit and Control Association*) poolt 31. juulil 2002. a.

Tallinnas, 7. oktoobril 2002. a.

Sulev Luiga
juhatuse esimees
KPMG Estonia