AS Sertifitseerimiskeskus

Sertifitseerimisteenuse osutaja infosüsteemi auditi raport

KPMG Estonia
31. august 2001
Dokument koosneb 9 leheküljest
SK 010831 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 teenuse 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;
- Ivo Koppelmaa, infosüsteemide audiitor (CISA sertifikaadi andmed – vt. Lisa 2).

1.3 Auditi teostus

Viisime auditi läbi ajavahemikus 13. augustist kuni 30. augustini 2001. a. Tööde käigus tutvusime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna ja dokumentatsiooniga, intervjueerisime võtmeisikuid ning viisime läbi muid kontrolliprotseduure, mille hulka kuulus ka osalemine juursertifikaadi võtmete loomise protseduuri juures vaatlejatena.

1.4 Auditi tulemust mõjutavad asjaolud

Johtuvalt asjaolust, et infosüsteemi auditi läbiviimine on sertifitseerimisteenuse osutamise eeltingimuseks, ei olnud meil võimalik tutvuda tööprotsessidega, mis käivituvad alles teenuse osutamisel. Seega polnud meil ka võimalik kontrollida töökorralduse vastavust AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtetele.

AS-i Sertifitseerimiskeskus infotehnoloogiline keskkond pole veel lõplikult valminud, lõpetamisel on serveriruumi remont ja seadmete paigaldamine.

Valmimata on infosüsteemi taasteplaan, kuna see on otstarbekas koostada pärast infosüsteemi töölerakendamist ja olukorra stabiliseerumist.

Audit tugines olulises osas dokumentatsiooni analüüsile. Ettevõtte infotehnoloogilise keskkonna juhtimist, infosüsteemi turvalisust ning sertifitseerimisteenuse osutamist puudutav dokumentatsioon on koostatud põhjalikkusega, mis ei anna alust kahelda ettevõtte suutlikkuses pakkuda kvaliteetset sertifitseerimisteenust.

1.5 Audiitori otsus

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

Oleme seisukohal, et AS-is Sertifitseerimiskeskus rajatav infosüsteem vastab Teede- ja sideministri 3. oktoobri 2000. a. määruses nr. 83 "Teenuse osutajate infosüsteemide auditeerimise kord" esitatud nõuetele. Me ei näe takistusi määruse nõuetele vastava infosüsteemi töölerakendamisele lähemal ajal.

AS-i Sertifitseerimiskeskus töötajate hinnangul saavutab ettevõte valmisoleku sertifitseerimisteenuse pakkumiseks oktoobris 2001. Meie arvamuse kohaselt on valmisoleku saavutamine oktoobris 2001 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 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.

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 infosüsteemi arhitektuur, komponendid ja lähiajal kavandatud arendused vastavad dokumenteeritud sertifitseerimispõhimõtetele. Organisatsiooniliste meetmete ja töökorralduse vastavust sertifitseerimispõhimõtetele ei ole enne teenuse osutamise alustamist võimalik hinnata.

2.5 Vastavus ajatembelduspõhimõtetele

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

AS Sertifitseerimiskeskus ei soovi hetkel ajatempliteenust pakkuda. Seetõttu ei sisaldanud audit nimetatud vastavuse kontrolli.

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 ja §19 esitatud kriteeriumitele ning on võimeline täitma §22 loetletud sertifitseerimisteenuse 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 ettevõtte hankeprotsessi vastavust standardi EVS-ISO/IEC 12207 osale 5.1, keskendudes sertifitseerimistarkvara hankele. Meie hinnangul viidi nimetatud protsess üldjoontes läbi standardile vastavalt. Leidsime mõningaid lahknevusi standardi kitsalt spetsifitseeritud nõuete osas, mille täitmine väikesearvulise töötajaskonnaga ettevõttes ei olekski põhjendatud.

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 infoturbe strateegia ja poliitikate 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 on infoturbe korraldamisel järginud standardis esitatud head tava.

Kontrollisime võtmehalduse kavandatud protsesse vastavalt standardi ISO/TR 13569 osale 7.4. Oleme arvamusel, et AS Sertifitseerimiskeskus on järginud nimetatud standardi osas esitatud nõudeid. Lahtiseks jäi küsimus Baltimore UniCERT tarkvara vastavusest standardis viidatud teistele ISO standarditele. Samas lisab tarkvarale usaldusväärsust sellele omistatud ITSEC E3 turvatase.

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 osale PO4 – "Määratleda IT organisatsioon ja seosed". Jõudsime järeldusele, et PO4 ärinõue "tarnida IT teenuseid" ja ka PO4 juhtimiseesmärgid on saavutatavad. Lahknevus standardist ilmnes juhtimiseesmärgis 3 "Organisatsiooniliste saavutuste läbivaatus", mis meie arvates on antud suurusega ettevõtte kontekstis ebaoluline.

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 *"Requirements on CA practice"* nõuetele (välja arvatud 7.2 *"PKI – Key management life cycle"*, mille kattis ISO/TR 13569 osa 7.4). Jõudsime seisukohale, et AS Sertifitseerimiskeskus on järginud nimetatud standardis esitatud head tava vastavalt 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

Ivo Koppelmaa
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) üleandmiseks 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 infosüsteemide audiitorite Ivo Koppelmaa ja Jüri Tirmaste poolt ajavahemikus 13. augustist kuni 30. augustini 2001. a.

Tallinnas, 31. augustil 2001. a.

Kalle Tarien
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 vastavad KPMG Estonia infosüsteemide audiitorid Ivo Koppelmaa ja Jüri Tirmaste Korra §-s 5 esitatud audiitori sõltumatuse nõudele.

Samuti kinnitame, et Ivo Koppelmaa omas auditi läbiviimise ajal kehtivat infosüsteemide sertifitseeritud audiitori CISA sertifikaati nr. 0023034, mis on välja antud Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (*Information Systems Audit and Control Association*) poolt 11. septembril 2000. a.

Tallinnas, 31. augustil 2001. a.

Andres Root
juhatuse esimees
KPMG Estonia