



AS Sertifitseerimiskeskus

Sertifitseerimisteenuse ja
ajatempliteenuse osutaja
infosüsteemi auditi raport

Advisory

Oktoober 2009

Aruanne sisaldab 6 lehekülge

Lisad koosnevad 2 lehest

SK STO auditi aruanne 2009

Sisukord

1	Kokkuvõte	1
1.1	Auditi eesmärk	1
1.2	Audiitori andmed	1
1.3	Auditi teostus	1
1.4	Audiitori otsus	1
2	Hinnangud ja järeldused	2
2.1	Kvaliteetne ja turvaline teenus	2
2.2	Vastavus õigusaktidele	2
2.3	Põhjendused mittevastavustele	2
2.4	Vastavus sertifitseerimispõhimõtetele	2
2.5	Vastavus ajatembelduspõhimõtetele	2
2.6	„Digitaalallkirja seaduse” kohustuste täidetus	3
2.7	EVS-ISO/IEC 12207	3
2.8	EVS-ISO/IEC TR 13335 ja ISO/TR 13569	3
2.9	COBIT	3
2.10	Spetsiifilised nõuded	4
2.11	Muud tehnilised normid	4

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 (edaspidi TO) infosüsteemi auditeerimist, eesmärgiga määrata kindlaks infosüsteemi kasutuskõlblikkus ning vastavus õigusaktidega kehtestatud nõuetele ja normidele.

1.2 Audiitori andmed

Auditi viis läbi KPMG Baltics AS *Manager* Janno Kase (CISA sertifikaat nr. 0541738, välja antud Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni poolt 15. september 2005. a.).

1.3 Auditi teostus

Viisime auditi läbi ajavahemikus 28. september - 31. oktoober 2009. a. Tööde käigus tutvusime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna ja dokumentatsiooniga, intervjuerisime võtmeisikuid, jälgisime tööprotsesse ning viisime läbi muid kontrolliprotseduure.

1.4 Audiitori otsus

Oleme auditeerinud AS-i Sertifitseerimiskeskus infotehnoloogilist keskkonda. Arvame, et meie auditi ulatus 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 ettevõtte 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 selgunud.

2.4 Vastavus sertifitseerimispehimoetetele

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

Ettevõtte infosüsteem, organisatsioon ja töökorraldus vastavad olulises osas dokumenteeritud sertifitseerimispehimoetetele.

2.5 Vastavus ajatembelduspõhimoetetele

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

Ettevõtte infosüsteem, organisatsioon ja töökorraldus vastavad dokumenteeritud ajatembelduspõhimõtetele.

2.6 „Digitaalallkirja seaduse” kohustuste täidetud

Kontrollitakse teenuse osutaja kohustuste täidetust vastavalt «Digitaalallkirja seadusele».

Meie hinnangul vastab AS Sertifitseerimiskeskus Digitaalallkirja seaduse §18 lõige (1) punktis 1, §25 punktis 1, §19, §21, §26 ja §29 esitatud kriteeriumitele ning on võimeline täitma §22 loetletud sertifitseerimisteenuse osutaja ja §28 loetletud ajatempliteenuse osutaja kohustusi. AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted vastavad Digitaalallkirja seaduse §20 nõuetele ning ajatembelduspõhimõtted seaduse §27 nõuetele.

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 6.2 (Konfiguratsiooni halduse protsess). Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib sertifitseerimisteenuse ja ajatempliteenuse konfiguratsiooni halduse protsessi osas standardis esitatud põhimõtteid.

2.8 EVS-ISO/IEC TR 13335 ja ISO/TR 13569

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 13335-1,2,3 “Infoturbe halduse suunised” osadele 10.2 (Turvateadlikkus) ja 10.3 (Turvakoolitus). Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib turvateadlikkuse ja turvakoolituse valdkonnas olulises osas standardis esitatud põhimõtteid.

Kontrollisime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna vastavust standardi ISO/TR 13569 osadele 7.10 (Faksid), 7.11 (E-mail) ja 7.12 (Paberdokument). Oleme arvamusel, et AS Sertifitseerimiskeskus järgib sertifitseerimisteenuse ja ajatempliteenuse osutamisel standardis esitatud põhimõtteid fakside, e-mailide ja paberdokumentide kasutamise ja säilitamise osas.

2.9 COBIT

Kontrollitakse TO infosüsteemi vastavust materjalile «COBIT (Control Objectives for Information and Related Technology) Auditi suunised, juuli 2000, 3. redaktsioon. Infosüsteemide auditi ja juhtimise fondi väljaanne.» Aruandes märgitakse, millistele osadele vastavust kontrolliti.

Kontrollisime vastavust COBIT-i protsessile AI6 (HE6) (Hallata muutusi). Jõudsime järeldusele, et AS-i Sertifitseerimiskeskuse võimekus hallata muudatusi vastab olulises osas standardi nõuetele.

2.10 Spetsiifilised nõuded

Kontrollitakse TO infosüsteemi vastavust spetsiifilistele sertifitseerimis- või ajatempliteenuse osutamise 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 6 “Liability” ja 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.

Kontrollisime ettevõtte infoturbevalduse vastavust standardi EVS-ISO/IEC 17799:2003 osale 5 (Varade liigitamine ja ohje)”. Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib olulises osas nimetatud standardis esitatud nõudeid varade liigitamisele ja ohjele.

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

Lugupidamisega

(allkirjastatud digitaalselt)

Taivo Epner
KPMG Baltics AS Partner

(allkirjastatud digitaalselt)

Janno Kase
KPMG Baltics AS Manager, CISA

Lisa 1: Kinnitus auditi toimumise kohta antud ajavahemikul

Lisa 2: Koopia audiitori CISA sertifikaadist