AS Sertifitseerimiskeskus

Sertifitseerimisteenuse ja ajatempliteenuse osutaja infosüsteemi auditi raport

Advisory
Oktoober 2011
Aruanne sisaldab 6 lehekülge
SK STO auditi aruanne 2011

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 (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 OÜ *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 23. september - 28. oktoober 2011. 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 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.***

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 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 infosüsteem, organisatsioon ja töökorraldus vastavad dokumenteeritud ajatembelduspõhimõtetele.

2.6 „Digitaalallkirja seaduse" kohustuste täidetus

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 kriteeriumidele 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 osadele 5.3 (Arendusprotsess) ja 6.3 (Kvaliteedi tagamise protsess). Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib sertifitseerimisteenuse ja ajatempliteenuse hooldusprotsessi 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" osale 11 (Järeltegevused). Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib infoturbe eesmärkide, strateegia ja poliitika valdkonnas olulises osas standardis esitatud põhimõtteid.
Kontrollisime AS-i Sertifitseerimiskeskus infotehnoloogilise keskkonna vastavust standardi ISO/TR 13569 osadele 7.7 (Tarkvara) ja 7.8 (Inimfaktorid). Oleme arvamusel, et AS Sertifitseerimiskeskus järgib arvutite osas sertifitseerimisteenuse ja ajatempliteenuse osutamisel standardis esitatud põhimõtteid.

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 PO9 (Riskide hindamine) ja DS4 (Tagada pidev teenus). Jõudsime järeldusele, et AS-i Sertifitseerimiskeskuse võimekus operatsioone hallata vastab olulises osas standardi nõuetele.

2.10 Muud tehnilised normid

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

Kontrollisime ettevõtte infoturbehalduse vastavust standardi EVS-ISO/IEC 17799:2003 osale 9 (Pääsu reguleerimine). Jõudsime järeldusele, et AS Sertifitseerimiskeskus järgib olulises osas nimetatud standardis esitatud nõudeid organisatsioonilisele turbele.

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

Lugupidamisega

(allkirjastatud digitaalselt)

Andris Jegers
KPMG Baltics OÜ Partner

(allkirjastatud digitaalselt)

Janno Kase
KPMG Baltics OÜ Manager, CISA

Lisa 1: Kinnitus auditi toimumise kohta antud ajavahemikul

Lisa 2: Koopia audiitori CISA sertifikaadist