AS Sertifitseerimiskeskus

Certification service and time-stamping service provider's information system audit report

RAS
October 2007
This report contains 8 pages
Appendices comprise 1 pages
Certification service and time-stamping service provider IT system audit report.doc

Contents

Summary

1.1 The objective of the audit

Our objective is to carry out AS Sertifitseerimiskeskus information systems` audit pursuant to Minister of Transport and Communications October 3, 2000 regulation No. 83 "Service providers` information systems` auditing procedure". The regulation regulates the auditing process of the certification and time-stamping service provider's (hereinafter TO) information system, with the objective to determine the usability and correspondence of the information system to the requirements and norms set by legal acts.

1.2 Auditor's data

The audit was carried out by KPMG Baltics AS *Senior Adviser* Kitty Mamers (CISA certificate No. 0540258, issued by Information Systems` Audit and Management Association on May 17, 2005).

1.3 Audit implementation

We carried out the audit between September 26 – October 29, 2007. During the works, we familiarised ourselves with AS Sertifitseerimiskeskus information tehnological environment and documentation, interviewed the key personnel, surveyed the work processes and carried out other checking procedures.

1.4 Auditor's decision

We have audited AS Sertifitseerimiskeskus information technological environment. We think that the extent of our audit gives sufficient basis for expression of opinion regarding AS Sertifitseerimiskeskus information systems.

We are of the opinion that AS Sertifitseerimiskeskus information system corresponds to requirements provided in Minister of Transport and Communications` October 3, 2000 regulation No. 83 "Service providers` information systems` auditing procedure."

Evaluations and conclusions

The structure of this part of report "Evaluations and conclusions" follows the structure of „Service providers` information systems auditing procedure" §15 confirmed by Minister of Transport and Communications October 3, 2000 regulation No. 83. The regulation has been cited in ***italics and bold.***

1.5 High- quality and safe service

It is checked whether TO has been applied relevant professional accuracy to guarantee a high-quality and safe service.

Considering AS Sertifitseerimiskeskus personnel policy, qualifications of employees, thoroughness and conservatism in critical areas, set work methods and existing information technological environment, we are of the opinion that the company is capable of guaranteeing certification service and time-stamping service quality and safety on a continuous basis.

1.6 Correspondence to legal acts

The correspondence of TO information system is checked against «Digital signature act», «Personal data protection act», «Data bases` act» and the requirements provided by other legal acts and paragraph 16 of this regulation.

The existing information technological environment and planned developments of it do not pose hindrances to guaranteeing correspondence of the information system to valid legal acts. AS Sertifitseerimiskeskus information system corresponds to the specified requirements provided in paragraph 16 of the regulation.

1.7 Reasons of non- correspondence

Non-correspondence to requirements provided in this paragraph clause 2 [in clause 2.2 of this report] ***must be substantiated in the audit report.***

The named non-correspondence did not appear during the audit.

1.8 Correspondence to certification principles

TO information system is checked, including correspondence of organisation and working order to documented certification principles.

Enterprises` information system, organisation and working order correspond to significant extent to documented certification principles.

1.9 Correspondence to time-stamping principles

Correspondence of time-stamping provider's information system, including organisation and working order correspondence to documented time-stamping principles is checked.

The enterprise's information system, organisation and working order correspond to documented time-stamping principles.

1.10 Fulfilment of „Digital signature act" requirement

Fulfilment of service provider's obligations according to «Digital signature act».

We confirm that AS Sertifitseerimiskeskus corresponds to criteria provided in Digital signature act §18 subsection (1) in clause 1, §25 in clause 1, §19, §21, §26 and §29 and has been capable of fulfilling obligations of certification service provider listed in §22 and time-stamping service provider listed in §28. AS Sertifitseerimiskeskus certification principles correspond to Digital signature act §20 requirements and Time-stamping principles act §27 requirements.

1.11 EVS-ISO/IEC 12207

Correspondence of service provider's information system is checked against standard EVS-ISO/IEC 12207, noting in report, and which parts of standard correspondence were checked.

We checked correspondence to standard EVS-ISO/IEC 12207 part 5.4 "Operation process". We reached the conclusion that AS Sertifitseerimiskeskus follows principles prescribed in the standard in operation process of software of certification service and time-stamping service.

1.12 EVS-ISO/IEC TR 13335 and ISO/TR 13569

The correspondence of service provider's information system safety is checked against standards EVS-ISO/IEC TR 13335-1,2,3 and ISO/TR 13569, noting in report, and which parts of standard correspondence were checked.

We checked the correspondence of the enterprise's information safety procedure to standard EVS ISO/IEC TR 13335-3 "Information safety administration directions. Part 3: Information safety administration methods" chapter 7 "IT security objectives, strategy and policies". We reached the conclusion that AS Sertifitseerimiskeskus follows significantly information safety organisation principles provided in standard.

We checked correspondence of AS Sertifitseerimiskeskus information technological environment to standard ISO/TR 13569 chapter 7 "Safety methods implementation" to part 7.2 "Logical access". We are of the opinion that providing logical access of the software of certification service and time-stamping services AS Sertifitseerimiskeskus follows the requirements provided in the named standard.

Correspondence of TO information system is checked against material «COBIT (Control Objectives for Information and Related Technology) Audit guidelines, April 1998, 2. redaction. Information system's audit and management fund publication.» The report notes which parts of standard correspondence were checked.

We checked correspondence to COBIT process DS5 "Ensure systems security". We came to the conclusion that AS Sertifitseerimiskeskus has followed significantly standard requirements.

1.14 Specific requirements

Correspondence of TO information systems is checked against specific requirements connected with certification and time-stamping service provision; note in report, which parts of standard correspondence were checked.

We checked correspondence to standard ETSI TS 101 456 "*Policy requirements for certification authorities issuing qualified certificates*" part 6 "*Obligations and liability*" and part 7 "*Requirements on CA practice*" and standard ETSI TS 102 023 "*Policy requirements for time-stamping authorities*" part 7 "*Requirements on TSA practices*" requirements.

We reached the opinion that AS Sertifitseerimiskeskus has followed the good practice provided in the named standards according to expediency proceeding from the size of the company, first and foremost, following the legal acts valid in Estonia.

1.15 Other technical norms

Correspondence of TO information systems is checked against the technical norms and requirements provided in legal acts significant from the standpoint of provision of service.

We checked correspondence of the enterprise's information safety procedure to standard EVS-ISO/IEC 17799:2003 part 6 "Personnel security". We reached the conclusion that AS Sertifitseerimiskeskus follows significantly the requirements provided in the named standard.

At the time the audit was carried out, there were no significant technical norms and requirements from the standpoint of provision of service set by legal acts.

Yours faithfully

(signed digitally)

Kitty Mamers
AS KPMG Baltics Senior Adviser, CISA

Annex 1: Confirmation of the taking place of the audit during the given period

Annex 2: Copy of CISA certificate of auditor