ISKE audit manual

Version 1.4
January 2017

Contents

1. Introduction

This document provides guidelines for performing ISKE audits. Generally, performing an ISKE audit has been regulated by the 20 December 2007 Government of the Republic regulation No. 252, *The system of security measures for information systems* (hereinafter the ISKE regulation). This document clarifies auditing aspects which have not been provided in the regulation or which require clarification, and provides additional guidelines for ordering and performing ISKE audits.

2. Definitions and abbreviations

CISA – Certified Information Systems Auditor
Information system – technical system processing, storing, or transmitting data, along with the means, resources, and processes needed for its normal operation
ISACA – Information Systems Audit and Control Association
ISKE – three-level IT baseline security system of information systems

3. The purpose of an ISKE audit

3.1 The purpose of an ISKE audit is to evaluate, whether the ISKE security measures have been implemented in maintaining the state data store(s) included in the state information system.

4. Ordering an ISKE audit

4.1 Chief processors of state data stores included in the state information system must order an ISKE audit based on the data store security level pursuant to section 9^1 of the ISKE regulation;

4.1.1 The chief processor of a data store with a data store security level of "H" must carry out an independent audit of the implementation of the security management system once every two years.

4.1.2 The chief processor of a data store with a data store security level of "M" must carry out an independent audit of the implementation of the security management system once every three years.

4.1.3 The chief processor of a data store with a data store security level of "L" must carry out an independent audit of the implementation of the security management system once every four years.

4.2 It is recommended that an ISKE audit be ordered by the department of internal audit and/or by the internal auditor. If the agency does not have a department of internal audit or internal auditor, the ISKE audit must be ordered by another department, e.g. general department.

4.3 If the data of the audited data store is processed in several locations, the chief processor of the data store must prescribe in the contract notice or agreement the minimum number of locations where the audit is performed. If data is processed in three locations or less, the audit must cover all the locations.

4.4 If the agency has previously ordered a conformity audit, they must note in the contract notice document whether the previously audited modules must be included in compiling the sample of modules for the new audit.

5. Performing an ISKE audit

5.1 An audit on the implementation of the security management system must be carried out in that part of the information system where the data of the data store is being processed.

5.2 The following works must be performed in the course of the audit:

5.2.1 checking whether the performed inventory of information assets corresponds to the requirements;

5.2.2 checking the assignment of security classes and security levels;

5.2.3 checking the selection of security measures subject to implementation, i.e. whether the security measures were selected pursuant to the requirements provided in the ISKE implementation manual;

5.2.4 checking the implementation of all security measures subject to implementation (see clause 6);

5.2.5 An ISKE audit may be ordered for several data stores simultaneously; in that case, the final report of the audit must give an assessment to all data stores.

5.3 Prior to performing the works provided in clause 5.2, the auditor must examine the information security documentation of the agency and assess whether the agency has met the prerequisites for successfully carrying out an ISKE audit. Should it become evident in examining the documentation that the agency lacks the prerequisites for successfully carrying out an audit, the auditor must advise not continuing with the ISKE audit project and allow the agency to rectify the initial deficiencies and order an ISKE audit after this.

5.4 For successfully carrying out an ISKE audit, the agency should have documented and performed the following works: updating the inventory of information assets, mapping

the data stores and assigning chief users for these, assigning security classes and security levels to data stores, assigning security levels to other information assets, preparing lists of standard modules and security measures subject to implementation, and implementing security measures. The list of security measures must be in a written form and include at least the standard modules based on ISKE, security measures subject to implementation, and persons responsible for each measure, e.g. the IT department, external partner, authorised processor, etc. If an agency has more than one data store, these works must be performed for each data store.

5.5 When ordering ISKE audits to data stores at different times, the so-called common components (e.g. organisational side, physical safety) do not have to be audited multiple times, if less time has passed since the previous audit than what is required by the data stores auditing obligation (see clause 4.1).

5.6 An audit must generally be carried out by means of documentation and an on-site inspection. If the on-site inspection cannot be performed, the auditor may use the documents of the service provider and inspection of security certificates.

6. Inspection of implementation of security measures subject to implementation

6.1 The implementation of the following modules must be checked in the course of the ISKE audit's inspection of implementation of security measures:

6.1.1 implementation of all security measures belonging to the B1.0 module;

6.1.2 additionally, implementation of modules subject to implementation previously chosen by the auditor from module groups B1, B2, B3, B4 and B5, and the security measures subject to implementation included in these. Two modules must be chosen from each of the module groups mentioned. Modules are chosen by using the simple random sampling method. A representative of the party who orders should be present while compiling the random sample. If a representative of the party who orders was not present while the sample was compiled, this must be noted in the final audit report. A total of ten additional modules must be selected using this method;

6.1.3 additionally, implementation of modules subject to implementation previously chosen by the auditor from module groups B1, B2, B3, B4 and B5, and the security measures subject to implementation included in these. The most significant module must be selected from each of the module groups mentioned. The auditor may consider the opinion of the representative of the party who orders when assessing significance. A total of five additional modules must be selected using this method;

6.2 When ordering and performing an audit for several data stores simultaneously and/or data stores of several agencies simultaneously, the modules described in clause 6.1 must be chosen separately for each data store subject to auditing.

6.3 An auditor may also assess the implementation of other security measures if needed or if the party who orders the ISKE audit requests it.

6.4 If the on-site inspection cannot be performed, the auditor may inspect the documents and security certificates of the service provider.

7. Requirements for the performer of the ISKE audit works

7.1 When carrying out the audit, the chief processor of a data store must ensure that, during the time the audit is carried out, the auditor has at least one of the following certificates:

7.1.1 Certificate of Certified Information Systems Auditor, CISA issued by the Information Systems Audit and Control Association.
The validity of the certificate can be checked at https://www.isaca.org/Pages/default.aspx;

7.1.2 All auditors with a ISO 27001 who can be found in the register provided on the webpage of International Register of Certificated Auditors http://www.irca.org/home.html are accepted;

7.1.3 an ISO 27001 IT certified auditor certificate based on Grundschutz, issued by the Federal Office for Information Security of Germany (Bundesamt für Sicherheit in der Informationstechnik).

7.2 Upon performing the work, the auditor must adhere to the Code of Professional Ethics, standards, guidelines, rules of procedure and good practices of the Information Systems Audit and Control Association (hereinafter ISACA) in Estonian http://www.eisay.ee/ and English http://www.isaca.org;

7.3 Several auditors with a certificate provided in clause 7.1 may participate in an ISKE audit project. In that case, one auditor is chosen who manages the work of the audit team and is responsible for the works performed in the course of the audit and signs the final audit report.

7.4 The auditor must be independent of the auditable.

7.4.1 An auditor may not be a person who has consulted the institution in the field that is being audited within two years prior to the audit.

7.4.2 The independence of the auditor and each specialist in the audit team (including other auditors involved in the audit) must be verified by a document signed by the auditor and specialist in the audit team, respectively.

7.5 The auditor must keep the information obtained while performing their duties confidential

7.6 The auditor may use the work of other specialists in the ISKE audit, while conforming to the ISACA standards.

8. Requirements for preparing an ISKE report

8.1 In the final report of the audit, the auditor must assess the following:

8.1.1 whether the inventory of information assets has been carried out pursuant to the requirements provided in the ISKE implementation manual, including whether the presence of connections between the information assets and data stores was evaluated, the correspondence of the information assets included in the documentation to the actual situation was checked, etc.;

8.1.2 whether the security classes/security levels assigned to the data store(s) are relevant, i.e. whether the owners of the data stores were interviewed to clarify requirements provided to the data store by laws, agreements, other internal processes, and importance of consequences. In addition, the procedures for assigning a security class and regular inspection are checked, etc.;

8.1.3 whether the security measures subject to implementation have been chosen correctly and in accordance with the requirements provided in the ISKE implementation manual, i.e. it is checked whether appropriate ISKE standard modules have been chosen for controlling the measures according to the information assets, whether the choice of measures is correct and complete, etc.;

8.1.4 whether all security measures subject to implementation have been implemented, i.e. whether interviews are being carried out, documentation prepared in the agency is being examined and tests being carried out to check the

implementation. The status of each tested measure is documented along with the auditor's assessment.

8.2 In addition, the auditor must note in the final report all such security measures which have not been implemented and/or which have partially not been implemented if not implementing these and/or not implementing these partially may result in high-level risks for maintaining the data store.

8.3 For each security measure provided in clause 8.2, the auditor must give recommendations on how such measures should be implemented.

8.4 The ISKE audit report must provide the names of all the auditors and specialists involved in the ISKE audit.

8.5 An annex to the ISKE final report must include a table of all audited security measures where the auditor must note, among other things, for each security measure whether the security measure has been implemented, has been partially implemented, has not been implemented, cannot be implemented or will not be implemented.

8.6 If the chief processor has decided not to implement a security measure, i.e. its status is 'will not be implemented' provided in the previous clause, the auditor must assess the sufficiency of the reasoning for not implementing that security measure and the risks stemming from not implementing it, and then give their assessment on whether not implementing the security measure is reasoned.

8.7 For each partially implemented security measure, the auditor must write down the deficiency/deficiencies regarding which the security measure has not been implemented and give recommendations for eliminating such deficiency/deficiencies.

8.8 The annexes to the final report of the ISKE audit must include all other documents created by the audit team in the course of the ISKE audit, and for each remark or recommendation, evidence which the remark or recommendation is based on must be referred to, e.g. outcomes of tests and observations, interviews, examined guidelines and rules of procedures that the auditor based their assessment on.

8.9 The final report of the ISKE audit must be formulated in a way which would allow the auditable to create extra cells after the measures which have partially not been implemented and not implemented, where they can insert the person responsible for implementing the measure, and the term.

9. Activities after the audit

9.1 The chief processor is obligated to implement the measures marked as having a high risk level in the final report of the audit as soon as possible, and implement the rest of the measures which have not been implemented during a reasonable time period.

9.2 Immediately after implementing the measures with a high risk level, an ex-post audit of their implementation must be ordered, and this can be carried out by an auditor who adheres to the requirements provided in clause 7.1. The ex-post audit may be performed by the same auditor who carried out the initial audit.

9.3 Only those security measures for which note(s) regarding a high risk level were made must be audited in the course of the ex-post audit.

9.4 Within one month after the audit was carried out, the chief processor of the data store must note the outcome of the ISKE audit in the state information system of information system management.