INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemi teostusjuhis

Information technology
Security techniques
Information security management system
Implementation guidance
(ISO/IEC 27003:2010)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard EVS-ISO/IEC 27003:2011 „Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemi teostusjuhis“ sisaldab rahvusvahelise standardi ISO/IEC 27003:2010 „Information technology - Security techniques – Information security management system implementation guidance“ identset ingliskeelset teksti.

Standard EVS-ISO/IEC 27003:2011 on kinnitatud Eesti Standardikeskuse 01.03.2011 käskkirjaga ja on jõustunud sellekohase teate avaldamisel EVS Teatajas.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

This Estonian Standard EVS-ISO/IEC 27003:2011 consists of the identical English text of the International Standard ISO/IEC 27003:2010 “Information technology - Security techniques - Information security management system implementation guidance”.

This standard is ratified with the order of Estonian Centre for Standardisation dated 01.03.2011 and is endorsed with the notification published in the official bulletin of the Estonian Centre for Standardisation.

This standard is available from the Estonian Centre for Standardisation.

Käsitlusala

Standard keskendub olulistele aspektidele, mida tuleb arvestada infoturbe halduse süsteemi (ISMS) edukaks kavandamiseks ja teostamiseks kooskõlas standardiga ISO/IEC 27001:2005. Selles kirjeldatakse ISMSi spetsifitseerimise ja kavandamise protsessi algatamisest kuni rakendusplaanide koostamiseni. Samuti kirjeldatakse protsessi, millega saadakse ISMSi teostamisele juhtkonna heakskiit, määrab ISMSi rakendamise projekti (mida selles standardis nimetatakse ISMS projektiks) ning annab juhiseid selle kohta, kuidas plaanida ISMS projekti, mis tuleneb lõplikust ISMS projekti rakendusplaanist.

See standard on mõeldud kasutamiseks ISMSi tegevatele organisatsioonidele. See on kohaldatav igat tüüpi ja iga suurusega organisatsioonidele (näiteks äriettevõtetele, riigiasutustele, mittetulundusühingutele). Iga organisatsiooni keerukus ja riskid on ainulaadsed ning konkreetsed nõuded suunavad ISMSi teostamist. Standardis mainitud tegevused on lihtsustatavad ja neid saab kohaldada ka väiksematele organisatsioonidele. Suuremastaabilised või keerukad organisatsioonid võivad standardis mainitud tegevuste toimivaks haldamiseks vajada mitmekihilist organiseerimis- või haldussüsteemi. Mõlemal juhul aga saab asjakohaseid tegevusi plaanida seda standardit rakendades.

Standard annab soovitusi ja seletusi ega määra kindlaks mingeid nõudeid. See on mõeldud kasutamiseks koos standarditega ISO/IEC 27001:2005 ja ISO/IEC 27002:2005, kuid mitte ISO/IEC 27001:2005 nõuete ega ISO/IEC 27002:2005 soovituste muutmiseks ega vähendamiseks. Standardile vastavust ei ole vaja deklareerida.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27003 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The purpose of this International Standard is to provide practical guidance in developing the implementation plan for an Information Security Management System (ISMS) within an organization in accordance with ISO/IEC 27001:2005. The actual implementation of an ISMS is generally executed as a project.

The process described within this International Standard has been designed to provide support of the implementation of ISO/IEC 27001:2005; (relevant parts from Clauses 4, 5, and 7 inclusive) and document:

a) the preparation of beginning an ISMS implementation plan in an organization, defining the organizational structure for the project, and gaining management approval,

b) the critical activities for the ISMS project and,

c) examples to achieve the requirements in ISO/IEC 27001:2005.

By using this International Standard the organization will be able to develop a process for information security management, giving stakeholders the assurance that risks to information assets are continuously maintained within acceptable information security bounds as defined by the organization.

This International Standard does not cover the operational activities and other ISMS activities, but covers the concepts on how to design the activities which will result after the ISMS operations begin. The concept results in the final ISMS project implementation plan. The actual execution of the organizational specific part of an ISMS project is outside the scope of this International Standard.

The implementation of the ISMS project should be carried out using standard project management methodologies (for more information please see ISO and ISO/IEC Standards addressing project management).

Information technology — Security techniques — Information security management system implementation guidance

1 Scope

This International Standard focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in this International Standard as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

This International Standard is intended to be used by organizations implementing an ISMS. It is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations) of all sizes. Each organization's complexity and risks are unique, and its specific requirements will drive the ISMS implementation. Smaller organizations will find that the activities noted in this International Standard are applicable to them and can be simplified. Large-scale or complex organizations might find that a layered organization or management system is needed to manage the activities in this International Standard effectively. However, in both cases, the relevant activities can be planned by applying this International Standard.

This International Standard gives recommendations and explanations; it does not specify any requirements. This International Standard is intended to be used in conjunction with ISO/IEC 27001:2005 and ISO/IEC 27002:2005, but is not intended to modify and/or reduce the requirements specified in ISO/IEC 27001:2005 or the recommendations provided in ISO/IEC 27002:2005. Claiming conformity to this International Standard is not appropriate.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2009, ISO/IEC 27001:2005 and the following apply.

3.1
ISMS project
structured activities undertaken by an organization to implement an ISMS