INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemid
Ülevaade ja sõnavara

Information technology
Security techniques
Information security management systems
Overview and vocabulary

(ISO/IEC 27000:2009)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard EVS-ISO/IEC 27000:2010 “Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Ülevaade ja sõnavara” sisaldab rahvusvahelise standardi ISO/IEC 27000:2009 “Information technology - Security techniques - Information security management systems - Overview and vocabulary” identset ingliskeelset teksti.

Standard EVS-ISO/IEC 27000:2010 on kinnitatud Eesti Standardikeskuse 05.08.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teataja 2010. aasta septembrikuu numbris.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

This Estonian Standard EVS-ISO/IEC 27000:2010 consists of the identical English text of the International Standard ISO/IEC 27000:2009 “Information technology - Security techniques - Information security management systems - Overview and vocabulary”.

This standard is ratified with the order of Estonian Centre for Standardisation dated 05.08.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

The standard is available from Estonian Centre for Standardisation.

Käsitlusala

Käesolev standard annab

a) ülevaate ISMS-i standardiperest;

b) sissejuhatuse infoturbe halduse süsteemidesse (ISMS);

c) PDCA-protsessi (“plaanida, teha, kontrollida, tegutseda”) lühikirjelduse;

d) terminid ja määratlused ISMS-i standardiperes kasutamiseks.

See standard on rakendatav igat liiki organisatsioonides (näiteks äriettevõtetes, riigiasutustes, mitte-tulunduslikes organisatsioonides).

ICS 01.040.35 Infotehnoloogia. Kontoriseadmed (sõnavara); **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 27000 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

0 Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1 SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets and prepare for an independent assessment of their ISMS applied to the protection of information, such as financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties.

0.2 ISMS family of standards

The ISMS family of standards[1)] is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology — Security techniques*:

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

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

— ISO/IEC 27002:2005, *Code of practice for information security management*

— ISO/IEC 27003, *Information security management system implementation guidance*

— ISO/IEC 27004, *Information security management — Measurement*

— ISO/IEC 27005:2008, *Information security risk management*

— ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems*

— ISO/IEC 27007, *Guidelines for information security management systems auditing*

— ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

NOTE The general title "*Information technology — Security techniques*" indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

— ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

1) Standards identified throughout this subclause with no release year indicated are still under development.