EESTI STANDARD EVS-EN ISO/IEC 27000:2017

# INFOTEHNOLOOGIA. TURBEMEETODID. INFOTURBE HALDUSE SÜSTEEMID. ÜLEVAADE JA SÕNAVARA

# Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

| | |
|---|---|
| See Eesti standard EVS-EN ISO/IEC 27000:2017 sisaldab Euroopa standardi EN ISO/IEC 27000:2017 ingliskeelset teksti. | This Estonian standard EVS-EN ISO/IEC 27000:2017 consists of the English text of the European standard EN ISO/IEC 27000:2017. |
| Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas | This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation. |
| Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 22.02.2017. | Date of Availability of the European standard is 22.02.2017. |
| Standard on kättesaadav Eesti Standardikeskusest. | The standard is available from the Estonian Centre for Standardisation. |

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 01.040.35, 03.100.70, 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

**EN ISO/IEC 27000**

February 2017

ICS 01.040.35; 03.100.70; 35.030

English Version

# Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016)

Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016)

Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie (ISO/IEC 27000:2016)

This European Standard was approved by CEN on 26 January 2017.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels**

## European foreword

The text of ISO/IEC 27000:2016 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27000:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

### Endorsement notice

The text of ISO/IEC 27000:2016 has been approved by CEN as EN ISO/IEC 27000:2017 without any modification.

# Contents

Page

**Foreword** v

**0 Introduction** 1
0.1 Overview 1
0.2 ISMS family of standards 1
0.3 Purpose of this International Standard 2

**1 Scope** 2

**2 Terms and definitions** 2

**3 Information security management systems** 14
3.1 General 14
3.2 What is an ISMS? 14
3.2.1 Overview and principles 14
3.2.2 Information 15
3.2.3 Information security 15
3.2.4 Management 15
3.2.5 Management system 16
3.3 Process approach 16
3.4 Why an ISMS is important 16
3.5 Establishing, monitoring, maintaining and improving an ISMS 17
3.5.1 Overview 17
3.5.2 Identifying information security requirements 17
3.5.3 Assessing information security risks 18
3.5.4 Treating information security risks 18
3.5.5 Selecting and implementing controls 18
3.5.6 Monitor, maintain and improve the effectiveness of the ISMS 19
3.5.7 Continual improvement 19
3.6 ISMS critical success factors 20
3.7 Benefits of the ISMS family of standards 20

**4 ISMS family of standards** 21
4.1 General information 21
4.2 Standards describing an overview and terminology 22
4.2.1 ISO/IEC 27000 (this International Standard) 22
4.3 Standards specifying requirements 22
4.3.1 ISO/IEC 27001 22
4.3.2 ISO/IEC 27006 22
4.4 Standards describing general guidelines 22
4.4.1 ISO/IEC 27002 22
4.4.2 ISO/IEC 27003 23
4.4.3 ISO/IEC 27004 23
4.4.4 ISO/IEC 27005 23
4.4.5 ISO/IEC 27007 23
4.4.6 ISO/IEC TR 27008 23
4.4.7 ISO/IEC 27013 24
4.4.8 ISO/IEC 27014 24
4.4.9 ISO/IEC TR 27016 24
4.5 Standards describing sector-specific guidelines 25
4.5.1 ISO/IEC 27010 25
4.5.2 ISO/IEC 27011 25
4.5.3 ISO/IEC TR 27015 25
4.5.4 ISO/IEC 27017 25
4.5.5 ISO/IEC 27018 26
4.5.6 ISO/IEC TR 27019 26
4.5.7 ISO 27799 26

**Annex A** (informative) **Verbal forms for the expression of provisions** 28
**Annex B** (informative) **Term and term ownership** 29
**Bibliography** 33

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This fourth edition cancels and replaces the third edition (ISO/IEC 27000:2014), which has been technically revised.

# Information technology — Security techniques — Information security management systems — Overview and vocabulary

## 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 including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

### 0.2 ISMS family of standards

The ISMS family of standards (see Clause 4) is intended to assist organizations of all types and sizes to implement and operate an ISMS and consists of the following International Standards, under the general title *Information technology — Security techniques* (given below in numerical order):

- ISO/IEC 27000, *Information security management systems — Overview and vocabulary*
- ISO/IEC 27001, *Information security management systems — Requirements*
- ISO/IEC 27002, *Code of practice for information security controls*
- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management — Measurement*
- ISO/IEC 27005, *Information security risk management*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ISO/IEC TR 27008, *Guidelines for auditors on information security controls*
- ISO/IEC 27009, *Sector-specific application* of *ISO/IEC 27001 — Requirements*
- ISO/IEC 27010, *Information security management for inter-sector and inter-organizational communications*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on* ISO/IEC 27002
- ISO/IEC 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

— ISO/IEC 27014, *Governance of information security*

— ISO/IEC TR 27015, *Information security management guidelines for financial services*

— ISO/IEC TR 27016, *Information security management — Organizational economics*

— ISO/IEC 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

— ISO/IEC 27018, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

— ISO/IEC 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

NOTE The general title "*Information technology — Security techniques*" indicates that these International 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, *Health informatics — Information security management in health using ISO/IEC 27002*

## 0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

The ISMS family of standards includes standards that

a) define requirements for an ISMS and for those certifying such systems,

b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS,

c) address sector-specific guidelines for ISMS, and

d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard

— cover commonly used terms and definitions in the ISMS family of standards,

— do not cover all terms and definitions applied within the ISMS family of standards, and

— do not limit the ISMS family of standards in defining new terms for use.

# 1 Scope

This International Standard provides the overview of information security management systems, and terms and definitions commonly used in the ISMS family of standards. This International Standard is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

# 2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.