SIST

SLOVENSKI STANDARD
oSIST ISO/IEC DIS 27000:2013

01-september-2013

Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti - Pregled in izrazje

Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Vue d'ensemble et vocabulaire

Ta slovenski standard je istoveten z: ISO/IEC DIS 27000

ICS:

01.040.35	Informacijska tehnologija. Pisarniški stroji (Slovarji)	Information technology. Office machines (Vocabularies)
35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

oSIST ISO/IEC DIS 27000:2013 **en,fr,de**

DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 27000

ISO/IEC JTC **1** Secretariat: **ANSI**

Voting begins on
2013-07-16

Voting terminates on
2013-10-16

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

[Revision of second edition (ISO/IEC 27000:2012)]

ICS 01.040.35; 35.040

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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*.

This third edition cancels and replaces the second edition (ISO/IEC 27000:2012).

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 FDIS27001, *Information security management systems — Requirements*
- ISO/IEC FDIS 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 management systems controls*
- ISO/IEC 27010, *Information security management guidelines 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 DTR 27016, *Information security management – Organizational economics*

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*

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;
- will 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.

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

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.

2.1
access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

2.2
analytical model
algorithm or calculation combining one or more **base** (2.10) and/or **derived measures** (2.22) with associated decision criteria

2.3
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

2.4
attribute
property or characteristic of an **object** (2.55) that can be distinguished quantitatively or qualitatively by human or automated means

[Adopted from ISO/IEC 15939:2007]

2.5
audit
systematic, independent and documented **process** (2.61) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2: “Audit evidence” and “audit criteria” are defined in ISO 19011.

2.6
audit scope

extent and boundaries of an **audit** (2.5)

[ISO 19011:2011]

2.7
authentication

provision of assurance that a claimed characteristic of an entity is correct

2.8
authenticity

property that an entity is what it is claims to be

2.9
availability

property of being accessible and usable upon demand by an authorized entity

2.10
base measure

measure (2.47) defined in terms of an **attribute** (2.4) and the method for quantifying it

[ISO/IEC 15939:2007]

Note: A base measure is functionally independent of other measures.

2.11
competence

ability to apply knowledge and skills to achieve intended results

2.12
confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or **processes** (2.61)

2.13
conformity

fulfillment of a **requirement** (2.63)

Note: The term “conformance” is synonymous but deprecated.

2.14
consequence

outcome of an **event** (2.25) affecting **objectives** (2.56)

[ISO Guide 73:2009]

Note 1: An event can lead to a range of consequences.

Note 2: A consequence can be certain or uncertain and in the context of information security is usually negative.

Note 3: Consequences can be expressed qualitatively or quantitatively.

Note 4: Initial consequences can escalate through knock-on effects.

2.15
continual improvement
recurring activity to enhance **performance** (2.59)

2.16
control
measure that is modifying **risk** (2.68)

[ISO Guide 73:2009]

Note 1: Controls include any process, policy, device,, practice, or other actions which modify risk.

Note 2: Controls may not always exert the intended or assumed modifying effect.

2.17
control objective
statement describing what is to be achieved as a result of implementing **controls** (2.16)

2.18
correction
action to eliminate a detected **nonconformity** (2.53)

2.19
corrective action
action to eliminate the cause of a **nonconformity** (2.53) and to prevent recurrence

2.20
data
collection of values assigned to **base measures** (2.10), **derived measures** (2.22) and/or **indicators** (2.30)

[ISO/IEC 15939:2007]

Note: This definition applies only within the context of ISO/IEC 27004:2009.

2.21
decision criteria
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result