

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemid
Nõuded

Information technology
Security techniques
Information security management systems
Requirements
(ISO/IEC 27001:2013 + Cor 1:2014)

EVS

EESTI STANDARDI EESSÕNA**NATIONAL FOREWORD**

<p>See Eesti standard EVS-ISO/IEC 27001:2014 „Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded“ sisaldab rahvusvahelise standardi ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements“ ja selle paranduse ISO/IEC 27001:2013/Cor 1:2014 identset ingliskeelset teksti.</p> <p>Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.</p> <p>Standard EVS-ISO/IEC 27001:2014 on jõustunud sellekohase teate avaldamisega EVS Teataja 2014. aasta oktoobrikuu numbris.</p> <p>Standard on kättesaadav Eesti Standardikeskusest.</p>	<p>This Estonian Standard EVS-ISO/IEC 27001:2014 consists of the identical English text of the International Standard ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements“ and its Corrigendum ISO/IEC 27001:2013/Cor 1:2014.</p> <p>Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian standard has been published by the Estonian Centre for Standardisation.</p> <p>This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.</p> <p>The standard is available from the Estonian Centre for Standardisation.</p>
--	---

Käsitlusala

See standard spetsifitseerib nõuded infoturbe halduse süsteemi rajamiseks, evituseks, käigushoiuks ja pidevaks täiustamiseks organisatsiooni kontekstis. Standard sisaldab ka nõudeid organisatsiooni vajadustele kohandatavaks infoturvariskide kaalutlemiseks ja käsitlemiseks. Selles standardis püstitatud nõuded on üldistuslikud ning on mõeldud kohandatavaks kõigile organisatsioonidele, sõltumata nende tüübist, suuruselt või iseloomust. Kui organisatsioon taotleb vastavust sellele standardile, ei tohi ta välistada ühtki peatükkides 4 kuni 10 spetsifitseeritud nõuet.

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

ICS 35.040

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:
Aru 10, 10317 Tallinn, Estonia; www.evs.ee; phone 605 5050; e-mail info@evs.ee

Contents

Page

Foreword	iv
0 Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	1
4.1 Understanding the organization and its context	1
4.2 Understanding the needs and expectations of interested parties	1
4.3 Determining the scope of the information security management system	1
4.4 Information security management system	2
5 Leadership	2
5.1 Leadership and commitment	2
5.2 Policy	2
5.3 Organizational roles, responsibilities and authorities	3
6 Planning	3
6.1 Actions to address risks and opportunities	3
6.2 Information security objectives and planning to achieve them	5
7 Support	5
7.1 Resources	5
7.2 Competence	5
7.3 Awareness	5
7.4 Communication	6
7.5 Documented information	6
8 Operation	7
8.1 Operational planning and control	7
8.2 Information security risk assessment	7
8.3 Information security risk treatment	7
9 Performance evaluation	7
9.1 Monitoring, measurement, analysis and evaluation	7
9.2 Internal audit	8
9.3 Management review	8
10 Improvement	9
10.1 Nonconformity and corrective action	9
10.2 Continual improvement	9
Annex A (normative) Reference control objectives and controls	10
Bibliography	23

0 Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003^[2], ISO/IEC 27004^[3] and ISO/IEC 27005^[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information technology — Security techniques — Information security management systems — Requirements

1 Scope

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in [Clauses 4](#) to [10](#) is not acceptable when an organization claims conformity to this International Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- a) interested parties that are relevant to the information security management system; and
- b) the requirements of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.