ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA September 2020

STN	**Informačné technológie Bezpečnostné metódy Požiadavky na orgány poskytujúce audit a certifikáciu pre systémy riadenia informačnej bezpečnosti**	**STN ISO/IEC 27006** 36 9795

Information technology
Security techniques
Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information
Techniques de sécurité
Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Informationstechnik
IT Sicherheitsverfahren
Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten

Táto norma obsahuje anglickú verziu ISO/IEC 27006: 2015, vrátane ISO/IEC 27006: 2015/Amd 1: 2020.

This standard includes the English version of ISO/IEC 27006: 2015, includes ISO/IEC 27006: 2015/Amd 1: 2020.

131590

Anotácia

Táto medzinárodná norma špecifikuje požiadavky a poskytuje usmernenie pre orgány poskytujúce audit a certifikáciu systému riadenia informačnej bezpečnosti (Information security management system – ISMS), doplňujúce požiadavky obsiahnuté v ISO/IEC 17021-1 a ISO/IEC 27001. Je určená predovšetkým na podporu akreditácie certifikačných orgánov poskytujúcich certifikáciu ISMS.

Požiadavky obsiahnuté v tejto medzinárodnej norme musia byť preukázané z hľadiska spôsobilosti a spoľahlivosti akýmkoľvek orgánom poskytujúcim certifikáciu ISMS a usmernenie obsiahnuté v tejto medzinárodnej norme poskytuje ďalší výklad týchto požiadaviek pre všetky subjekty poskytujúce certifikáciu ISMS.

Zmenou Amd1 sa upravujú ustanovenia časti prílohy B o výpočte dĺžky auditu.

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Principles **1**

5 General requirements **2**
5.1 Legal and contractual matters 2
5.2 Management of impartiality 2
5.2.1 IS 5.2 Conflicts of interest 2
5.3 Liability and financing 2

6 Structural requirements **2**

7 Resource requirements **2**
7.1 Competence of personnel 2
7.1.1 IS 7.1.1 General considerations 3
7.1.2 IS 7.1.2 Determination of Competence Criteria 3
7.2 Personnel involved in the certification activities 6
7.2.1 IS 7.2 Demonstration of auditor knowledge and experience 6
7.3 Use of individual external auditors and external technical experts 7
7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team 7
7.4 Personnel records 7
7.5 Outsourcing 7

8 Information requirements **8**
8.1 Public information 8
8.2 Certification documents 8
8.2.1 IS 8.2 ISMS Certification documents 8
8.3 Reference to certification and use of marks 8
8.4 Confidentiality 8
8.4.1 IS 8.4 Access to organizational records 8
8.5 Information exchange between a certification body and its clients 8

9 Process requirements **8**
9.1 Pre-certification activities 8
9.1.1 Application 8
9.1.2 Application review 9
9.1.3 Audit programme 9
9.1.4 Determining audit time 10
9.1.5 Multi-site sampling 10
9.1.6 Multiple management systems 11
9.2 Planning audits 11
9.2.1 Determining audit objectives, scope and criteria 11
9.2.2 Audit team selection and assignments 12
9.2.3 Audit plan 12
9.3 Initial certification 13
9.3.1 IS 9.3.1 Initial certification audit 13
9.4 Conducting audits 14
9.4.1 IS 9.4 General 14
9.4.2 IS 9.4 Specific elements of the ISMS audit 14
9.4.3 IS 9.4 Audit report 14
9.5 Certification decision 15
9.5.1 IS 9.5 Certification decision 15

9.6 Maintaining certification ... 15
9.6.1 General ... 15
9.6.2 Surveillance activities ... 15
9.6.3 Re-certification ... 16
9.6.4 Special audits ... 17
9.6.5 Suspending, withdrawing or reducing the scope of certification ... 17
9.7 Appeals ... 17
9.8 Complaints ... 17
9.8.1 IS 9.8 Complaints ... 17
9.9 Client records ... 17

10 Management system requirements for certification bodies ... 17
10.1 Options ... 17
10.1.1 IS 10.1 ISMS implementation ... 17
10.2 Option A: General management system requirements ... 17
10.3 Option B: Management system requirements in accordance with ISO 9001 ... 17

Annex A (informative) **Knowledge and skills for ISMS auditing and certification ... 18**

Annex B (normative) **Audit time ... 20**

Annex C (informative) **Methods for audit time calculations ... 25**

Annex D (informative) **Guidance for review of implemented ISO/IEC 27001:2013, Annex A controls ... 28**

Bibliography ... 35

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*.

ISO/IEC 27006 was prepared by the 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 27006:2011), which has been technically revised.

Introduction

ISO/IEC 17021-1 sets out criteria for bodies operating audit and certification of management systems. If such bodies are to be accredited as complying with ISO/IEC 17021-1 with the objective of auditing and certifying information security management systems (ISMS) in accordance with ISO/IEC 27001:2013, some additional requirements and guidance to ISO/IEC 17021-1 are necessary. These are provided by this International Standard.

The text in this International Standard follows the structure of ISO/IEC 17021-1 and the additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021-1 for ISMS certification are identified by the letters "IS".

The term "shall" is used throughout this International Standard to indicate those provisions which, reflecting the requirements of ISO/IEC 17021-1 and ISO/IEC 27001, are mandatory. The term "should" is used to indicate recommendation.

The primary purpose of this International Standard is to enable accreditation bodies to more effectively harmonize their application of the standards against which they are bound to assess certification bodies.

Throughout this International Standard, the terms "management system" and "system" are used interchangeably. The definition of a management system can be found in ISO 9000:2005. The management system as used in this International Standard is not to be confused with other types of systems, such as IT systems.

INTERNATIONAL STANDARD ISO/IEC 27006:2015(E)

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

1 Scope

This International Standard specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this International Standard provides additional interpretation of these requirements for any body providing ISMS certification.

NOTE This International Standard can be used as a criteria document for accreditation, peer assessment or other audit processes.

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 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

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

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*