



SLOVENSKI STANDARD
oSIST ISO/IEC 27006:2010
01-december-2010

Informacijska tehnologija - Varnostne tehnike - Zahteve za organe, ki izvajajo presoje in certificiranje sistemov upravljanja informacijske varnosti

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

Ta slovenski standard je istoveten z: ISO/IEC 27006:2007

ICS:

03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

oSIST ISO/IEC 27006:2010

en

INTERNATIONAL
STANDARD

**ISO/IEC
27006**

First edition
2007-03-01

**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*

Reference number
ISO/IEC 27006:2007(E)



© ISO/IEC 2007

ISO/IEC 27006:2007(E)**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2007

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles.....	2
5 General requirements.....	2
5.1 Legal and contractual matter.....	2
5.2 Management of impartiality	2
5.3 Liability and financing	3
6 Structural requirements	3
6.1 Organizational structure and top management.....	3
6.2 Committee for safeguarding impartiality	3
7 Resource requirements.....	3
7.1 Competence of management and personnel.....	3
7.2 Personnel involved in the certification activities	4
7.3 Use of individual external auditors and external technical experts	6
7.4 Personnel records	6
7.5 Outsourcing.....	6
8 Information requirements	6
8.1 Publicly accessible information	6
8.2 Certification documents.....	6
8.3 Directory of certified clients	7
8.4 Reference to certification and use of marks.....	7
8.5 Confidentiality	7
8.6 Information exchange between a certification body and its clients.....	7
9 Process requirements	7
9.1 General requirements.....	7
9.2 Initial audit and certification	11
9.3 Surveillance activities	15
9.4 Recertification	16
9.5 Special audits	16
9.6 Suspending, withdrawing or reducing scope of certification	16
9.7 Appeals	17
9.8 Complaints	17
9.9 Records of applicants and clients	17
10 Management system requirements for certification bodies	17
10.1 Options	17
10.2 Option 1 – Management system requirements in accordance with ISO 9001	17
10.3 Option 2 – General management system requirements	17
Annex A (informative) Analysis of a client organization’s complexity and sector-specific aspects	18
Annex B (informative) Example areas of auditor competence	21
Annex C (informative) Audit time.....	23
Annex D (informative) Guidance for review of implemented ISO/IEC 27001:2005, Annex A controls	29

ISO/IEC 27006:2007(E)**Foreword**

ISO (the International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO and 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 technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

ISO/IEC 17021 is an International Standard which sets out criteria for bodies operating audit and certification of organizations' management systems. If such bodies are to be accredited as complying with ISO/IEC 17021 with the objective of auditing and certifying Information Security Management Systems (ISMS) in accordance with ISO/IEC 27001:2005, some additional requirements and guidance to ISO/IEC 17021 are necessary. These are provided by this International Standard.

The text in this International Standard follows the structure of ISO/IEC 17021, and the additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 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 and ISO/IEC 27001, are mandatory. The term "should" is used to indicate those provisions which, although they constitute guidance for the application of the requirements, are expected to be adopted by a certification body.

One aim of this International Standard is to enable accreditation bodies to more effectively harmonise their application of the standards against which they are bound to assess certification bodies. In this context, any variation from the guidance by a certification body is an exception. Such variations will only be permitted on a case-by-case basis after the certification body has demonstrated to the accreditation body that the exception meets in some equivalent way the relevant requirements clause of ISO/IEC 17021, ISO/IEC 27001 and the intent of this International Standard.

NOTE 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 system, such as IT systems.

