# 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 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

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.