SLOVENSKI STANDARD
oSIST ISO/IEC 27005:2011

01-februar-2011

Informacijska tehnologija - Varnostne tehnike - Upravljanje tveganj informacijske varnosti

Information technology -- Security techniques -- Information security risk management

Technologies de l'information -- Techniques de sécurité -- Gestion des risques en sécurité de l'information

Ta slovenski standard je istoveten z: ISO/IEC 27005:2008

ICS:

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding

oSIST ISO/IEC 27005:2011   **en,fr**

INTERNATIONAL STANDARD

ISO/IEC 27005

First edition
2008-06-15

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion du risque en sécurité de l'information

Reference number
ISO/IEC 27005:2008(E)

© ISO/IEC 2008

ISO/IEC 27005:2008(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.

Contents

Page

ISO/IEC 27005:2008(E)

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 27005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27005 cancels and replaces ISO/IEC TR 13335-3:1998, and ISO/IEC TR 13335-4:2000, of which it constitutes a technical revision.

v

ISO/IEC 27005:2008(E)

Introduction

This International Standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS according to ISO/IEC 27001. However, this International Standard does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.