



**SLOVENSKI STANDARD**  
**oSIST ISO/IEC FDIS 27005:2011**  
**01-april-2011**

---

**Informacijska tehnologija - Varnostne tehnike - Upravljanje tveganj informacijske varnosti**

Information technology - Security techniques - Information security risk management

Technologies de l'information - Techniques de sécurité - Management du risque de la sécurité de l'information

**Ta slovenski standard je istoveten z: ISO/IEC FDIS 27005**

---

**ICS:**

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding
--------	---------------------------------------	---------------------------------------

**oSIST ISO/IEC FDIS 27005:2011**                      **en**



FINAL  
DRAFT

INTERNATIONAL  
STANDARD

ISO/IEC  
FDIS  
27005

ISO/IEC JTC 1

Secretariat: **ANSI**

Voting begins on:  
**2011-02-21**

Voting terminates on:  
**2011-04-21**

---

---

## Information technology — Security techniques — Information security risk management

*Technologies de l'information — Techniques de sécurité — Gestion des  
risques liés à la sécurité de l'information*

Please see the administrative notes on page iii

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number  
ISO/IEC FDIS 27005:2011(E)

© ISO/IEC 2011

**ISO/IEC FDIS 27005:2011(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.

**Copyright notice**

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to 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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

# Contents

Page

Foreword .....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions .....	1
4 Structure of this International Standard .....	5
5 Background.....	6
6 Overview of the information security risk management process .....	7
7 Context establishment.....	10
7.1 General considerations.....	10
7.2 Basic Criteria .....	10
7.2.1 Risk management approach .....	10
7.2.2 Risk evaluation criteria .....	10
7.2.3 Impact criteria .....	11
7.2.4 Risk acceptance criteria .....	11
7.3 Scope and boundaries.....	12
7.4 Organization for information security risk management .....	12
8 Information security risk assessment.....	13
8.1 General description of information security risk assessment .....	13
8.2 Risk identification.....	13
8.2.1 Introduction to risk identification .....	13
8.2.2 Identification of assets.....	14
8.2.3 Identification of threats.....	14
8.2.4 Identification of existing controls.....	15
8.2.5 Identification of vulnerabilities .....	15
8.2.6 Identification of consequences.....	16
8.3 Risk analysis.....	17
8.3.1 Risk analysis methodologies .....	17
8.3.2 Assessment of consequences.....	18
8.3.3 Assessment of incident likelihood .....	18
8.3.4 Level of risk determination.....	19
8.4 Risk evaluation .....	19
9 Information security risk treatment.....	20
9.1 General description of risk treatment .....	20
9.2 Risk modification.....	22
9.3 Risk retention.....	23
9.4 Risk avoidance .....	23
9.5 Risk sharing .....	23
10 Information security risk acceptance.....	24
11 Information security risk communication and consultation.....	24
12 Information security risk monitoring and review.....	25
12.1 Monitoring and review of risk factors .....	25
12.2 Risk management monitoring, reviewing and improving .....	26

## ISO/IEC FDIS 27005:2011(E)

<b>Annex A</b> (informative) <b>Defining the scope and boundaries of the information security risk management process</b> .....	<b>28</b>
<b>A.1</b> <b>Study of the organization</b> .....	<b>28</b>
<b>A.2</b> <b>List of the constraints affecting the organization</b> .....	<b>29</b>
<b>A.3</b> <b>List of the legislative and regulatory references applicable to the organization</b> .....	<b>31</b>
<b>A.4</b> <b>List of the constraints affecting the scope</b> .....	<b>31</b>
<b>Annex B</b> (informative) <b>Identification and valuation of assets and impact assessment</b> .....	<b>33</b>
<b>B.1</b> <b>Examples of asset identification</b> .....	<b>33</b>
<b>B.1.1</b> <b>The identification of primary assets</b> .....	<b>33</b>
<b>B.1.2</b> <b>List and description of supporting assets</b> .....	<b>34</b>
<b>B.2</b> <b>Asset valuation</b> .....	<b>38</b>
<b>B.3</b> <b>Impact assessment</b> .....	<b>41</b>
<b>Annex C</b> (informative) <b>Examples of typical threats</b> .....	<b>42</b>
<b>Annex D</b> (informative) <b>Vulnerabilities and methods for vulnerability assessment</b> .....	<b>45</b>
<b>D.1</b> <b>Examples of vulnerabilities</b> .....	<b>45</b>
<b>D.2</b> <b>Methods for assessment of technical vulnerabilities</b> .....	<b>48</b>
<b>Annex E</b> (informative) <b>Information security risk assessment approaches</b> .....	<b>50</b>
<b>E.1</b> <b>High-level information security risk assessment</b> .....	<b>50</b>
<b>E.2</b> <b>Detailed information security risk assessment</b> .....	<b>51</b>
<b>E.2.1</b> <b>Example 1 Matrix with predefined values</b> .....	<b>52</b>
<b>E.2.2</b> <b>Example 2 Ranking of Threats by Measures of Risk</b> .....	<b>54</b>
<b>E.2.3</b> <b>Example 3 Assessing a value for the likelihood and the possible consequences of risks</b> .....	<b>54</b>
<b>Annex F</b> (informative) <b>Constraints for risk modification</b> .....	<b>56</b>
<b>Annex G</b> (informative) <b>Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011</b> .....	<b>58</b>
<b>Bibliography</b> .....	<b>68</b>

## 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 second edition cancels and replaces the first edition (ISO/IEC 27005:2008) which has been technically revised.

**ISO/IEC FDIS 27005:2011(E)****Introduction**

This International Standard provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001. However, this International Standard does not provide any specific method 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.