INTERNATIONAL STANDARD

ISO/IEC 27005

Second edition
2011-06-01

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

Reference number
ISO/IEC 27005:2011(E)

© ISO/IEC 2011

COPYRIGHT PROTECTED DOCUMENT

©   ISO/IEC 2011

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

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, review and improvement 26
Annex A (informative) Defining the scope and boundaries of the information security risk management process 28
A.1 Study of the organization 28
A.2 List of the constraints affecting the organization 29
A.3 List of the legislative and regulatory references applicable to the organization 31
A.4 List of the constraints affecting the scope 31
Annex B (informative) Identification and valuation of assets and impact assessment 33
B.1 Examples of asset identification 33
B.1.1 The identification of primary assets 33
B.1.2 List and description of supporting assets 34
B.2 Asset valuation 38
B.3 Impact assessment 41
Annex C (informative) Examples of typical threats 42
Annex D (informative) Vulnerabilities and methods for vulnerability assessment 45
D.1 Examples of vulnerabilities 45
D.2 Methods for assessment of technical vulnerabilities 48
Annex E (informative) Information security risk assessment approaches 50
E.1 High-level information security risk assessment 50
E.2 Detailed information security risk assessment 51
E.2.1 Example 1 Matrix with predefined values 52
E.2.2 Example 2 Ranking of Threats by Measures of Risk 54
E.2.3 Example 3 Assessing a value for the likelihood and the possible consequences of risks 54
Annex F (informative) Constraints for risk modification 56
Annex G (informative) Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011 58
Bibliography 68

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.

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.

INTERNATIONAL STANDARD **ISO/IEC 27005:2011(E)**

Information technology — Security techniques — Information security risk management

1 Scope

This International Standard provides guidelines for information security risk management.

This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this International Standard.

This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*