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

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

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 PROTECTED DOCUMENT**

© ISO/IEC 2008

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.....	3
5 Background	3
6 Overview of the information security risk management process.....	4
7 Context establishment	7
7.1 General considerations	7
7.2 Basic Criteria	7
7.3 The scope and boundaries	8
7.4 Organization for information security risk management.....	9
8 Information security risk assessment	9
8.1 General description of information security risk assessment.....	9
8.2 Risk analysis	10
8.2.1 Risk identification	10
8.2.2 Risk estimation	14
8.3 Risk evaluation.....	16
9 Information security risk treatment	17
9.1 General description of risk treatment.....	17
9.2 Risk reduction	19
9.3 Risk retention	20
9.4 Risk avoidance	20
9.5 Risk transfer	20
10 Information security risk acceptance	21
11 Information security risk communication	21
12 Information security risk monitoring and review	22
12.1 Monitoring and review of risk factors.....	22
12.2 Risk management monitoring, reviewing and improving.....	23
Annex A (informative) Defining the scope and boundaries of the information security risk management process	25
A.1 Study of the organization.....	25
A.2 List of the constraints affecting the organization	26
A.3 List of the legislative and regulatory references applicable to the organization.....	28
A.4 List of the constraints affecting the scope	28
Annex B (informative) Identification and valuation of assets and impact assessment.....	30
B.1 Examples of asset identification	30
B.1.1 The identification of primary assets	30
B.1.2 List and description of supporting assets	31
B.2 Asset valuation	35
B.3 Impact assessment.....	38
Annex C (informative) Examples of typical threats	39
Annex D (informative) Vulnerabilities and methods for vulnerability assessment	42

D.1 Examples of vulnerabilities 42

D.2 Methods for assessment of technical vulnerabilities..... 45

Annex E (informative) Information security risk assessment approaches 47

E.1 High-level information security risk assessment 47

E.2 Detailed information security risk assessment 48

E.2.1 Example 1 Matrix with predefined values 48

E.2.2 Example 2 Ranking of Threats by Measures of Risk..... 50

E.2.3 Example 3 Assessing a value for the likelihood and the possible consequences of risks 51

Annex F (informative) Constraints for risk reduction 53

Bibliography 55

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.

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.

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

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*