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

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

© ISO/IEC 2008 – All rights reserved