

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*

**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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

## Contents

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