

INTERNATIONAL  
STANDARD

ISO/IEC  
27005

Third edition  
2018-07

---

---

**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 27005:2018(E)

© ISO/IEC 2018



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [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 document</b> .....	<b>1</b>
<b>5 Background</b> .....	<b>2</b>
<b>6 Overview of the information security risk management process</b> .....	<b>3</b>
<b>7 Context establishment</b> .....	<b>5</b>
7.1 General considerations.....	5
7.2 Basic criteria.....	6
7.2.1 Risk management approach.....	6
7.2.2 Risk evaluation criteria.....	6
7.2.3 Impact criteria.....	6
7.2.4 Risk acceptance criteria.....	7
7.3 Scope and boundaries.....	7
7.4 Organization for information security risk management.....	8
<b>8 Information security risk assessment</b> .....	<b>8</b>
8.1 General description of information security risk assessment.....	8
8.2 Risk identification.....	9
8.2.1 Introduction to risk identification.....	9
8.2.2 Identification of assets.....	9
8.2.3 Identification of threats.....	10
8.2.4 Identification of existing controls.....	10
8.2.5 Identification of vulnerabilities.....	11
8.2.6 Identification of consequences.....	12
8.3 Risk analysis.....	12
8.3.1 Risk analysis methodologies.....	12
8.3.2 Assessment of consequences.....	13
8.3.3 Assessment of incident likelihood.....	14
8.3.4 Level of risk determination.....	15
8.4 Risk evaluation.....	15
<b>9 Information security risk treatment</b> .....	<b>16</b>
9.1 General description of risk treatment.....	16
9.2 Risk modification.....	18
9.3 Risk retention.....	19
9.4 Risk avoidance.....	19
9.5 Risk sharing.....	19
<b>10 Information security risk acceptance</b> .....	<b>20</b>
<b>11 Information security risk communication and consultation</b> .....	<b>20</b>
<b>12 Information security risk monitoring and review</b> .....	<b>21</b>
12.1 Monitoring and review of risk factors.....	21
12.2 Risk management monitoring, review and improvement.....	22
<b>Annex A (informative) Defining the scope and boundaries of the information security risk management process</b> .....	<b>24</b>
<b>Annex B (informative) Identification and valuation of assets and impact assessment</b> .....	<b>28</b>
<b>Annex C (informative) Examples of typical threats</b> .....	<b>37</b>