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 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
Website: 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 document **1**
5 Background **2**
6 Overview of the information security risk management process **3**
7 Context establishment **5**
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
8 Information security risk assessment **8**
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
9 Information security risk treatment **16**
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
10 Information security risk acceptance **20**
11 Information security risk communication and consultation **20**
12 Information security risk monitoring and review **21**
12.1 Monitoring and review of risk factors 21
12.2 Risk management monitoring, review and improvement 22
Annex A (informative) **Defining the scope and boundaries of the information security risk management process** **24**
Annex B (informative) **Identification and valuation of assets and impact assessment** **28**
Annex C (informative) **Examples of typical threats** **37**