

INTERNATIONAL
STANDARD

ISO/IEC
27003

Second edition
2017-03

**Information technology — Security
techniques — Information security
management systems — Guidance**

*Technologies de l'information — Techniques de sécurité --Systèmes de
management de la sécurité de l'information — Lignes directrices*



Reference number
ISO/IEC 27003:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

| | |
|--|-----------|
| Foreword | iv |
| Introduction | v |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 Context of the organization | 1 |
| 4.1 Understanding the organization and its context..... | 1 |
| 4.2 Understanding the needs and expectations of interested parties..... | 3 |
| 4.3 Determining the scope of the information security management system..... | 4 |
| 4.4 Information security management system..... | 6 |
| 5 Leadership | 6 |
| 5.1 Leadership and commitment..... | 6 |
| 5.2 Policy..... | 8 |
| 5.3 Organizational roles, responsibilities and authorities..... | 9 |
| 6 Planning | 10 |
| 6.1 Actions to address risks and opportunities..... | 10 |
| 6.1.1 General..... | 10 |
| 6.1.2 Information security risk assessment..... | 12 |
| 6.1.3 Information security risk treatment..... | 15 |
| 6.2 Information security objectives and planning to achieve them..... | 18 |
| 7 Support | 21 |
| 7.1 Resources..... | 21 |
| 7.2 Competence..... | 22 |
| 7.3 Awareness..... | 23 |
| 7.4 Communication..... | 24 |
| 7.5 Documented information..... | 25 |
| 7.5.1 General..... | 25 |
| 7.5.2 Creating and updating..... | 27 |
| 7.5.3 Control of documented information..... | 28 |
| 8 Operation | 29 |
| 8.1 Operational planning and control..... | 29 |
| 8.2 Information security risk assessment..... | 31 |
| 8.3 Information security risk treatment..... | 31 |
| 9 Performance evaluation | 32 |
| 9.1 Monitoring, measurement, analysis and evaluation..... | 32 |
| 9.2 Internal audit..... | 33 |
| 9.3 Management review..... | 36 |
| 10 Improvement | 37 |
| 10.1 Nonconformity and corrective action..... | 37 |
| 10.2 Continual improvement..... | 40 |
| Annex A (informative) Policy framework | 42 |
| Bibliography | 45 |