
**Information technology — Security
techniques — Requirements
for bodies providing audit and
certification of information security
management systems**

*Technologies de l'information — Techniques de sécurité — Exigences
pour les organismes procédant à l'audit et à la certification des
systèmes de management de la sécurité de l'information*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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 | v |
| Introduction | vi |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 Principles | 1 |
| 5 General requirements | 2 |
| 5.1 Legal and contractual matters | 2 |
| 5.2 Management of impartiality | 2 |
| 5.2.1 IS 5.2 Conflicts of interest | 2 |
| 5.3 Liability and financing | 2 |
| 6 Structural requirements | 2 |
| 7 Resource requirements | 2 |
| 7.1 Competence of personnel | 2 |
| 7.1.1 IS 7.1.1 General considerations | 3 |
| 7.1.2 IS 7.1.2 Determination of Competence Criteria | 3 |
| 7.2 Personnel involved in the certification activities | 6 |
| 7.2.1 IS 7.2 Demonstration of auditor knowledge and experience | 6 |
| 7.3 Use of individual external auditors and external technical experts | 7 |
| 7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team | 7 |
| 7.4 Personnel records | 7 |
| 7.5 Outsourcing | 7 |
| 8 Information requirements | 8 |
| 8.1 Public information | 8 |
| 8.2 Certification documents | 8 |
| 8.2.1 IS 8.2 ISMS Certification documents | 8 |
| 8.3 Reference to certification and use of marks | 8 |
| 8.4 Confidentiality | 8 |
| 8.4.1 IS 8.4 Access to organizational records | 8 |
| 8.5 Information exchange between a certification body and its clients | 8 |
| 9 Process requirements | 8 |
| 9.1 Pre-certification activities | 8 |
| 9.1.1 Application | 8 |
| 9.1.2 Application review | 9 |
| 9.1.3 Audit programme | 9 |
| 9.1.4 Determining audit time | 10 |
| 9.1.5 Multi-site sampling | 10 |
| 9.1.6 Multiple management systems | 11 |
| 9.2 Planning audits | 11 |
| 9.2.1 Determining audit objectives, scope and criteria | 11 |
| 9.2.2 Audit team selection and assignments | 12 |
| 9.2.3 Audit plan | 12 |
| 9.3 Initial certification | 13 |
| 9.3.1 IS 9.3.1 Initial certification audit | 13 |
| 9.4 Conducting audits | 14 |
| 9.4.1 IS 9.4 General | 14 |
| 9.4.2 IS 9.4 Specific elements of the ISMS audit | 14 |
| 9.4.3 IS 9.4 Audit report | 14 |
| 9.5 Certification decision | 15 |
| 9.5.1 IS 9.5 Certification decision | 15 |