
**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*

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.

© ISO/IEC 2007

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
Web www.iso.org

Published in Switzerland

Contents

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles	2
5 General requirements	2
5.1 Legal and contractual matter	2
5.2 Management of impartiality	2
5.3 Liability and financing	3
6 Structural requirements	3
6.1 Organizational structure and top management	3
6.2 Committee for safeguarding impartiality	3
7 Resource requirements	3
7.1 Competence of management and personnel	3
7.2 Personnel involved in the certification activities	4
7.3 Use of individual external auditors and external technical experts	6
7.4 Personnel records	6
7.5 Outsourcing	6
8 Information requirements	6
8.1 Publicly accessible information	6
8.2 Certification documents	6
8.3 Directory of certified clients	7
8.4 Reference to certification and use of marks	7
8.5 Confidentiality	7
8.6 Information exchange between a certification body and its clients	7
9 Process requirements	7
9.1 General requirements	7
9.2 Initial audit and certification	11
9.3 Surveillance activities	15
9.4 Recertification	16
9.5 Special audits	16
9.6 Suspending, withdrawing or reducing scope of certification	16
9.7 Appeals	17
9.8 Complaints	17
9.9 Records of applicants and clients	17
10 Management system requirements for certification bodies	17
10.1 Options	17
10.2 Option 1 – Management system requirements in accordance with ISO 9001	17
10.3 Option 2 – General management system requirements	17
Annex A (informative) Analysis of a client organization’s complexity and sector-specific aspects	18
Annex B (informative) Example areas of auditor competence	21
Annex C (informative) Audit time	23
Annex D (informative) Guidance for review of implemented ISO/IEC 27001:2005, Annex A controls	29