
**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**

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



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos.....	v
Introduction.....	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Principes	1
5 Exigences générales	2
5.1 Domaine juridique et contractuel.....	2
5.2 Gestion de l'impartialité.....	2
5.2.1 SI 5.2 Conflits d'intérêts.....	2
5.3 Responsabilité et situation financière.....	2
6 Exigences structurelles	2
7 Exigences relatives aux ressources	2
7.1 Compétence du personnel.....	2
7.1.1 SI 7.1.1 Considérations générales.....	3
7.1.2 SI 7.1.2 Détermination des critères de compétence.....	3
7.2 Personnel intervenant dans les activités de certification.....	7
7.2.1 SI 7.2 Démonstration des connaissances et de l'expérience des auditeurs.....	7
7.3 Intervention d'auditeurs et d'experts techniques externes individuels.....	8
7.3.1 SI 7.3 Intervention d'auditeurs externes ou d'experts techniques externes au sein de l'équipe d'audit.....	8
7.4 Enregistrements relatifs au personnel.....	8
7.5 Externalisation.....	8
8 Exigences relatives aux informations	8
8.1 Informations publiques.....	8
8.2 Documents de certification.....	8
8.2.1 SI 8.2 Documents de certification SMSI.....	8
8.3 Référence à la certification et utilisation des marques.....	9
8.4 Confidentialité.....	9
8.4.1 SI 8.4 Accès aux enregistrements de l'organisation.....	9
8.5 Échange d'informations entre l'organisme de certification et ses clients.....	9
9 Exigences relatives aux processus	9
9.1 Activités préalables à la certification.....	9
9.1.1 Demande de certification.....	9
9.1.2 Revue de la demande.....	9
9.1.3 Programme d'audit.....	9
9.1.4 Détermination du temps d'audit.....	10
9.1.5 Échantillonnage multisite.....	11
9.1.6 Systèmes de management multiples.....	12
9.2 Planification des audits.....	12
9.2.1 Détermination des objectifs, du domaine d'application et des critères de l'audit.....	12
9.2.2 Constitution de l'équipe d'audit et affectation des missions.....	12
9.2.3 Plan d'audit.....	13
9.3 Certification initiale.....	14
9.3.1 SI 9.3.1 Audit de certification initiale.....	14
9.4 Réalisation des audits.....	15
9.4.1 SI 9.4 Généralités.....	15
9.4.2 SI 9.4 Éléments spécifiques de l'audit de SMSI.....	15
9.4.3 SI 9.4 Rapport d'audit.....	15
9.5 Décision de certification.....	16