
**Technologies de l'information —
Techniques de sécurité — Systèmes
de management de la sécurité de
l'information — Exigences**

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



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/CEI 2013

Droits de reproduction réservés. Sauf indication contraire, 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, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées 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 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

Version française parue en 2013

Publié en Suisse

Sommaire

Page

| | |
|--|-----------|
| Avant-propos | iv |
| 0 Introduction | v |
| 1 Domaine d'application | 1 |
| 2 Références normatives | 1 |
| 3 Termes et définitions | 1 |
| 4 Contexte de l'organisation | 1 |
| 4.1 Compréhension de l'organisation et de son contexte..... | 1 |
| 4.2 Compréhension des besoins et des attentes des parties intéressées..... | 1 |
| 4.3 Détermination du domaine d'application du système de management de la sécurité de l'information..... | 2 |
| 4.4 Système de management de la sécurité de l'information..... | 2 |
| 5 Leadership | 2 |
| 5.1 Leadership et engagement..... | 2 |
| 5.2 Politique..... | 2 |
| 5.3 Rôles, responsabilités et autorités au sein de l'organisation..... | 3 |
| 6 Planification | 3 |
| 6.1 Actions liées aux risques et opportunités..... | 3 |
| 6.2 Objectifs de sécurité de l'information et plans pour les atteindre..... | 5 |
| 7 Support | 5 |
| 7.1 Ressources..... | 5 |
| 7.2 Compétence..... | 6 |
| 7.3 Sensibilisation..... | 6 |
| 7.4 Communication..... | 6 |
| 7.5 Informations documentées..... | 6 |
| 8 Fonctionnement | 7 |
| 8.1 Planification et contrôle opérationnels..... | 7 |
| 8.2 Appréciation des risques de sécurité de l'information..... | 8 |
| 8.3 Traitement des risques de sécurité de l'information..... | 8 |
| 9 Évaluation des performances | 8 |
| 9.1 Surveillance, mesures, analyse et évaluation..... | 8 |
| 9.2 Audit interne..... | 8 |
| 9.3 Revue de direction..... | 9 |
| 10 Amélioration | 9 |
| 10.1 Non-conformité et actions correctives..... | 9 |
| 10.2 Amélioration continue..... | 10 |
| Annexe A (normative) Objectifs et mesures de référence | 11 |
| Bibliographie | 23 |