

This is a preview of "ISO/IEC 27001:2013[F...". [Click here to purchase the full version from the ANSI store.](#)

Deuxième édition
2013-10-01

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*

Numéro de référence
ISO/CEI 27001:2013(F)



© ISO/CEI 2013



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

This is a preview of "ISO/IEC 27001:2013[F...". [Click here to purchase the full version from the ANSI store.](#)

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

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27001 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 27001:2005), qui a fait l'objet d'une révision technique.

0 Introduction

0.1 Généralités

La présente Norme internationale a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

La présente Norme internationale peut être utilisée par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

L'ordre dans lequel les exigences sont présentées dans la présente Norme internationale ne reflète pas leur importance, ni l'ordre dans lequel elles doivent être mises en œuvre. Les éléments des listes sont énumérés uniquement à des fins de référence.

L'ISO/CEI 27000 décrit une vue d'ensemble et le vocabulaire des systèmes de management de la sécurité de l'information, en se référant à la famille des normes du système de management de la sécurité de l'information (incluant l'ISO/CEI 27003,^[2] l'ISO/CEI 27004^[3] et l'ISO/CEI 27005^[4]) avec les termes et les définitions qui s'y rapportent.

0.2 Compatibilité avec d'autres systèmes de management

La présente Norme internationale applique la structure de haut niveau, les titres de paragraphe identiques, le texte, les termes communs et les définitions fondamentales définies dans l'Annexe SL des Directives ISO/CEI, Partie 1, Supplément ISO consolidé, et, par conséquent, est compatible avec les autres normes de systèmes de management qui se conforment à l'Annexe SL.

Cette approche commune définie dans l'Annexe SL sera utile aux organisations qui choisissent de mettre en œuvre un système de management unique pour répondre aux exigences de deux ou plusieurs normes de systèmes de management.