NORME INTERNATIONALE

ISO/CEI 27001

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 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

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.

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

1 Domaine d'application

La présente Norme internationale spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. La présente Norme internationale comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. Les exigences fixées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité à la présente Norme internationale.

2 Références normatives

Les documents suivants, en tout ou partie, sont référencés de manière normative dans le présent document et sont indispensables à son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions fournis dans la norme ISO/CEI 27000 s'appliquent.

4 Contexte de l'organisation

4.1 Compréhension de l'organisation et de son contexte

L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui influent sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.

NOTE Déterminer ces enjeux revient à établir le contexte externe et interne de l'organisation étudié dans le paragraphe 5.3 de l'ISO 31000:2009.[5]

4.2 Compréhension des besoins et des attentes des parties intéressées

L'organisation doit déterminer:

a) les parties intéressées qui sont concernées par le système de management de la sécurité de l'information; et

b) les exigences de ces parties intéressées concernant la sécurité de l'information.

NOTE Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.

4.3 Détermination du domaine d'application du système de management de la sécurité de l'information

Pour établir le domaine d'application du système de management de la sécurité de l'information, l'organisation doit en déterminer les limites et l'applicabilité.

Lorsqu'elle établit ce domaine d'application, l'organisation doit prendre en compte:

a) les enjeux externes et internes auxquels il est fait référence en 4.1;

b) les exigences auxquelles il est fait référence en 4.2; et

c) les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.

Le domaine d'application doit être disponible sous forme d'information documentée.

4.4 Système de management de la sécurité de l'information

L'organisation doit établir, mettre en œuvre, tenir à jour et améliorer continuellement un système de management de la sécurité de l'information, conformément aux exigences de la présente Norme internationale.

5 Leadership

5.1 Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de la sécurité de l'information en:

a) s'assurant qu'une politique et des objectifs sont établis en matière de sécurité de l'information et qu'ils sont compatibles avec l'orientation stratégique de l'organisation;

b) s'assurant que les exigences liées au système de management de la sécurité de l'information sont intégrées aux processus métiers de l'organisation;

c) s'assurant que les ressources nécessaires pour le système de management de la sécurité de l'information sont disponibles;

d) communiquant sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences du système de management de la sécurité de l'information;

e) s'assurant que le système de management de la sécurité de l'information produit le ou les résultats escomptés;

f) orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du système de management de la sécurité de l'information;

g) promouvant l'amélioration continue; et

h) aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

5.2 Politique

La direction doit établir une politique de sécurité de l'information qui:

a) est adaptée à la mission de l'organisation;

b) inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit un cadre pour l'établissement de ces objectifs;

c) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information; et

d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information.

La politique de sécurité de l'information doit:

e) être disponible sous forme d'information documentée;

f) être communiquée au sein de l'organisation; et

g) être mise à la disposition des parties intéressées, le cas échéant.

5.3 Rôles, responsabilités et autorités au sein de l'organisation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

La direction doit désigner qui a la responsabilité et l'autorité de:

a) s'assurer que le système de management de la sécurité de l'information est conforme aux exigences de la présente Norme internationale; et

b) rendre compte à la direction des performances du système de management de la sécurité de l'information.

NOTE La direction peut également attribuer des responsabilités et autorités pour rendre compte des performances du système de management de la sécurité de l'information au sein de l'organisation.

6 Planification

6.1 Actions liées aux risques et opportunités

6.1.1 Généralités

Lorsqu'elle conçoit son système de management de la sécurité de l'information, l'organisation doit tenir compte des enjeux de 4.1 et des exigences de 4.2, et déterminer les risques et opportunités qui nécessitent d'être abordés pour:

a) s'assurer que le système de management de la sécurité de l'information peut atteindre le ou les résultats escomptés;

b) empêcher ou limiter les effets indésirables; et

c) appliquer une démarche d'amélioration continue.

L'organisation doit planifier:

d) les actions menées pour traiter ces risques et opportunités; et

e) la manière:

1) d'intégrer et de mettre en œuvre les actions au sein des processus du système de management de la sécurité de l'information; et

2) d'évaluer l'efficacité de ces actions.

6.1.2 Appréciation des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui:

a) établit et tient à jour les critères de risque de sécurité de l'information incluant:

   1) les critères d'acceptation des risques;

   2) les critères de réalisation des appréciations des risques de sécurité de l'information;

b) s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables;

c) identifie les risques de sécurité de l'information:

   1) applique le processus d'appréciation des risques de sécurité de l'information pour identifier les risques liés à la perte de confidentialité, d'intégrité et de disponibilité des informations entrant dans le domaine d'application du système de management de la sécurité de l'information; et

   2) identifie les propriétaires des risques;

d) analyse les risques de sécurité de l'information:

   1) apprécie les conséquences potentielles dans le cas où les risques identifiés en 6.1.2 c) 1) se concrétisaient;

   2) procède à une évaluation réaliste de la vraisemblance d'apparition des risques identifiés en 6.1.2 c) 1); et

   3) détermine les niveaux des risques;

e) évalue les risques de sécurité de l'information:

   1) compare les résultats d'analyse des risques avec les critères de risque déterminés en 6.1.2 a); et

   2) priorise les risques analysés pour le traitement des risques.

L'organisation doit conserver des informations documentées sur le processus d'appréciation des risques de sécurité de l'information.

6.1.3 Traitement des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information pour:

a) choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques;

b) déterminer toutes les mesures nécessaires à la mise en œuvre de(s) (l')option(s) de traitement des risques de sécurité de l'information choisie(s);

   NOTE Les organisations peuvent concevoir ces mesures, le cas échéant, ou bien les identifier à partir de n'importe quelle source.

c) comparer les mesures déterminées ci-dessus en 6.1.3 b) avec celles de l'Annexe A et vérifier qu'aucune mesure nécessaire n'a été omise;

   NOTE 1 L'Annexe A comporte une liste détaillée d'objectifs et de mesures. Les utilisateurs de la présente Norme internationale sont invités à se reporter à l'Annexe A pour s'assurer qu'aucune mesure nécessaire n'a été négligée.

   NOTE 2 Les objectifs sont implicitement inclus dans les mesures choisies. Les objectifs et les mesures énumérés dans l'Annexe A ne sont pas exhaustifs et des objectifs et des mesures additionnels peuvent s'avérer nécessaires.

d) produire une déclaration d'applicabilité contenant les mesures nécessaires (voir 6.1.3 b) et c)) et la justification de leur insertion, le fait qu'elles soient mises en œuvre ou non, et la justification de l'exclusion de mesures de l'Annexe A;

e) élaborer un plan de traitement des risques de sécurité de l'information; et

f) obtenir des propriétaires des risques l'approbation du plan de traitement des risques et l'acceptation des risques résiduels de sécurité de l'information.

L'organisation doit conserver des informations documentées sur le processus de traitement des risques de sécurité de l'information.

NOTE L'appréciation des risques de sécurité de l'information et le processus de traitement figurant dans la présente Norme internationale s'alignent sur les principes et les lignes directrices générales fournies dans l'ISO 31000.[5]

6.2 Objectifs de sécurité de l'information et plans pour les atteindre

L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information.

Les objectifs de sécurité de l'information doivent:

a) être cohérents avec la politique de sécurité de l'information;

b) être mesurables (si possible);

c) tenir compte des exigences applicables à la sécurité de l'information, et des résultats de l'appréciation et du traitement des risques;

d) être communiqués; et

e) être mis à jour quand cela est approprié.

L'organisation doit conserver des informations documentées sur les objectifs liés à la sécurité de l'information.

Lorsqu'elle planifie la façon d'atteindre ses objectifs de sécurité de l'information, l'organisation doit déterminer:

f) ce qui sera fait;

g) les ressources qui seront nécessaires;

h) qui sera responsable;

i) les échéances; et

j) la façon dont les résultats seront évalués.

7 Support

7.1 Ressources

L'organisation doit identifier et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue du système de management de la sécurité de l'information.

7.2 Compétence

L'organisation doit:

a) déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur les performances de la sécurité de l'information;

b) s'assurer que ces personnes sont compétentes sur la base d'une formation initiale ou continue ou d'une expérience appropriée;

c) le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité des actions entreprises; et

d) conserver des informations documentées appropriées comme preuves de ces compétences.

NOTE Les actions envisageables peuvent notamment inclure la formation, l'encadrement ou la réaffectation du personnel actuellement employé ou le recrutement, direct ou en sous-traitance, de personnes compétentes.

7.3 Sensibilisation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent:

a) être sensibilisées à la politique de sécurité de l'information;

b) avoir conscience de leur contribution à l'efficacité du système de management de la sécurité de l'information, y compris aux effets positifs d'une amélioration des performances de la sécurité de l'information; et

c) avoir conscience des implications de toute non-conformité aux exigences requises par le système de management de la sécurité de l'information.

7.4 Communication

L'organisation doit déterminer les besoins de communication interne et externe pertinents pour le système de management de la sécurité de l'information, et notamment:

a) sur quels sujets communiquer;

b) à quels moments communiquer;

c) avec qui communiquer;

d) qui doit communiquer; et

e) les processus par lesquels la communication doit s'effectuer.

7.5 Informations documentées

7.5.1 Généralités

Le système de management de la sécurité de l'information de l'organisation doit inclure:

a) les informations documentées exigées par la présente Norme internationale; et

b) les informations documentées que l'organisation juge nécessaires à l'efficacité du système de management de la sécurité de l'information.

NOTE L'étendue des informations documentées dans le cadre d'un système de management de la sécurité de l'information peut différer selon l'organisation en fonction de:

1) la taille de l'organisation, ses domaines d'activité et ses processus, produits et services;

