NORME INTERNATIONALE

ISO/CEI 27001

Première édition
2005-10-15

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

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

Numéro de référence
ISO/CEI 27001:2005(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 2007

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*.

0 Introduction

0.1 Généralités

La présente norme internationale a été élaborée pour fournir un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un SMSI (Système de Management de la Sécurité de l'Information). Il convient que l'adoption d'un SMSI relève d'une décision stratégique de l'organisme. La conception et la mise en œuvre du SMSI d'un organisme tiennent compte des besoins et des objectifs, des exigences de sécurité, des processus mis en œuvre, ainsi que la taille et de la structure de l'organisme. Ces éléments, ainsi que leurs systèmes connexes doivent évoluer avec le temps. Il convient d'adapter la mise en œuvre du SMSI conformément aux besoins de l'organisme, par exemple une situation simple requiert une solution SMSI tout aussi simple.

La présente norme internationale peut être utilisée pour des audits d'évaluation de la conformité, réalisés par des intervenants internes ou externes.

0.2 Approche processus

La présente norme internationale encourage l'adoption d'une approche processus pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI d'un organisme.

Tout organisme doit identifier et gérer de nombreuses activités de manière à fonctionner de manière efficace. Toute activité utilisant des ressources et gérée de manière à permettre la transformation d'éléments d'entrée en éléments de sortie, peut être considérée comme un processus. L'élément de sortie d'un processus constitue souvent l'élément d'entrée du processus suivant.

"L'approche processus" désigne l'application d'un système de processus au sein d'un organisme, ainsi que l'identification, les interactions et le management de ces processus.

L'approche processus pour le management de la sécurité de l'information présentée dans cette norme internationale incite ses utilisateurs à souligner l'importance de:

a) la compréhension des exigences relatives à la sécurité de l'information d'un organisme, et la nécessité de mettre en place une politique et des objectifs en matière de sécurité de l'information;

b) la mise en œuvre et l'exploitation des mesures de gestion des risques liés à la sécurité de l'information d'un organisme dans le contexte des risques globaux liés à l'activité de l'organisme;

c) la surveillance et le réexamen des performances et de l'efficacité du SMSI;

d) l'amélioration continue du système sur la base de mesures objectives.

La présente norme internationale adopte le modèle de processus "Planifier-Déployer-Contrôler-Agir" (PDCA) ou roue de Deming qui est appliqué à la structure de tous les processus d'un SMSI. La Figure 1 illustre comment un SMSI utilise comme élément d'entrée les exigences relatives à la sécurité de l'information et les attentes des parties intéressées, et comment il produit, par les actions et processus nécessaires, les résultats de sécurité de l'information qui satisfont ces exigences et ces attentes. La Figure 1 illustre également les liens entre les processus présentés dans les chapitres 4, 5, 6, 7 et 8.

L'adoption du modèle PDCA reflète également les principes fixés dans les lignes directrices de l'OCDE (2002)[1)] qui régissent la sécurité des systèmes et des réseaux d'information. La présente norme internationale fournit un modèle solide de mise en œuvre de ces principes dans les lignes directrices régissant l'appréciation des risques, la conception et la mise en œuvre de la sécurité, ainsi que la gestion et la réévaluation de cette même sécurité.

EXEMPLE 1

Une exigence pourrait être que toute violation de la sécurité de l'information n'entraînera aucun préjudice financier grave et/ou ne portera aucunement atteinte à l'organisme.

EXEMPLE 2

On pourrait s'attendre à ce que si un incident grave survient, par exemple le piratage informatique du site Web de commerce en ligne de l'organisme, celui-ci dispose de personnes suffisamment formées aux procédures convenables pour réduire l'impact de cet incident.

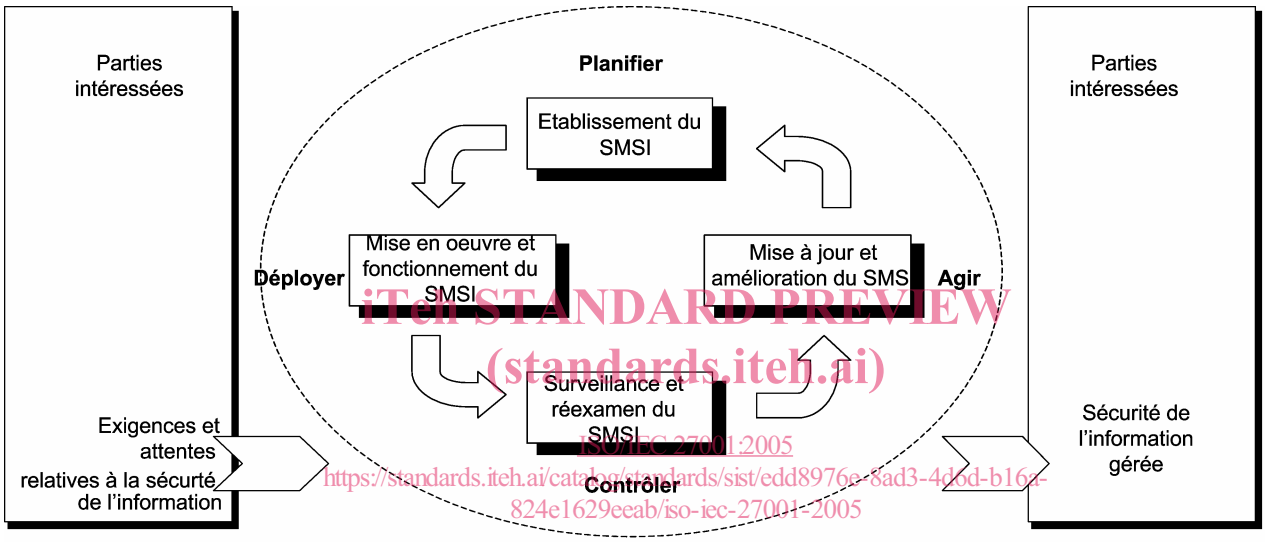

Figure 1 — Modèle PDCA appliqué aux processus SMSI

Planifier (établissement du SMSI)	Etablir la politique, les objectifs, les processus et les procédures du SMSI relatives à la gestion du risque et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformément aux politiques et aux objectifs globaux de l'organisme.
Déployer (mise en oeuvre et fonctionnement du SMSI)	Mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures du SMSI.
Contrôler (surveillance et réexamen du SMSI)	Evaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique et rendre compte des résultats à la direction pour réexamen.
Agir (mise à jour et amélioration du SMSI)	Entreprendre les actions correctives et préventives, sur la base des résultats de l'audit interne du SMSI et de la revue de direction, ou d'autres informations pertinentes, pour une amélioration continue dudit système.

1) Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information — Vers une culture de la sécurité. Paris: OCDE, Juillet 2002. www.oecd.org

0.3 Compatibilité avec d'autres systèmes de management

La présente norme internationale est alignée sur l'ISO 9001:2000 et l'ISO 14001:2004 afin de permettre une mise en œuvre et un fonctionnement cohérents et intégrés avec les autres normes de management. Un système de management convenablement conçu peut ainsi satisfaire les exigences de toutes ces normes. Le Tableau C.1 illustre la relation entre les articles et les paragraphes de la présente norme internationale et les normes ISO 9001:2000 et ISO 14001:2004.

La présente norme internationale a été conçue de manière à permettre à un organisme d'aligner ou d'intégrer son SMSI avec les exigences des autres systèmes de management.

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

IMPORTANT — La présente publication n'a pas pour objectif d'inclure toutes les dispositions nécessaires à un contrat. Les utilisateurs sont responsables de son application dans les conditions appropriées. La conformité à une norme ISO/CEI ne confère aucune exemption à la satisfaction des obligations légales.

1 Domaine d'application

1.1 Généralités

La présente Norme internationale couvre tous les types d'organismes (par exemple entreprises commerciales, organismes publics, organismes à but non lucratif). La présente Norme internationale spécifie les exigences relatives à l'établissement, à la mise en œuvre, au fonctionnement, à la surveillance et au réexamen, à la mise à jour et à l'amélioration d'un SMSI documenté dans le contexte des risques globaux liés à l'activité de l'organisme. Le présent document spécifie les exigences relatives à la mise en œuvre des mesures de sécurité adaptées aux besoins de chaque organisme ou à leurs parties constitutives.

Le SMSI est destiné à assurer le choix de mesures de sécurité adéquates et proportionnées qui protègent les actifs et donnent confiance aux parties intéressées.

NOTE 1 Il convient d'interpréter les références à "l'activité" dans la présente norme au sens large. Elles désignent les activités centrées sur les objectifs.

NOTE 2 L'ISO/CEI 17799 fournit des préconisations de mise en œuvre qui peuvent être utilisées lors de l'établissement des mesures.

1.2 Application

Les exigences fixées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à tout organisme, quels que soient son type, sa taille et sa nature. L'exclusion de l'une des exigences spécifiées aux Articles 4, 5, 6, 7 et 8 n'est pas acceptable lorsqu'un organisme revendique la conformité à la présente Norme internationale.

Toute exclusion des mesures jugée nécessaire pour satisfaire les critères d'acceptation du risque doit être justifiée et preuve doit être faite que les risques associés ont été acceptés par les personnes responsables. Lorsque des mesures sont exclues, les demandes de conformité à la présente Norme internationale ne sont acceptables que si ces exclusions n'affectent pas l'aptitude et/ou la responsabilité de l'organisme à assurer une sécurité de l'information conforme aux exigences de sécurité déterminées par l'appréciation du risque et les exigences réglementaires applicables.

NOTE Si un organisme dispose déjà d'un système opérationnel de management des processus métier (par exemple en rapport avec l'ISO 9001 ou l'ISO 14001), il est préférable, dans la plupart des cas de satisfaire les exigences de la présente norme dans le cadre de ce système de management existant.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. 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 17799:2005, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
actif
tout élément représentant de la valeur pour l'organisme

[ISO/CEI 13335-1:2004]

3.2
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

[ISO/CEI 13335-1:2004]

3.3
confidentialité
propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés

[ISO/CEI 13335-1:2004]

3.4
sécurité de l'information
protection de la confidentialité, de l'intégrité et de la disponibilité de l'information; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées

[ISO/CEI 17799:2005]

3.5
événement lié à la sécurité de l'information
occurrence identifiée d'un état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

[ISO/CEI TR 18044:2004]

3.6
incident lié à la sécurité de l'information
un ou plusieurs événements intéressant la sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information

[ISO/CEI TR 18044:2004]

3.7
système de management de la sécurité de l'information (SMSI)
partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information

NOTE Le système de management inclut l'organisation, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

3.8
intégrité
propriété de protection de l'exactitude et de l'exhaustivité des actifs

[ISO/CEI 13335-1:2004]

3.9
risque résiduel
risque subsistant après le traitement du risque

[ISO/CEI Guide 73:2002]

3.10
acceptation du risque
décision d'accepter un risque

[ISO/CEI Guide 73:2002]

3.11
analyse du risque
utilisation systématique d'informations pour identifier les sources et pour estimer le risque

[ISO/CEI Guide 73:2002]

3.12
appréciation du risque
ensemble du processus d'analyse du risque et d'évaluation du risque

[ISO/CEI Guide 73:2002]

3.13
évaluation du risque
processus de comparaison du risque estimé avec des critères de risque donnés pour en déterminer l'importance

[ISO/CEI Guide 73:2002]

3.14
management du risque
activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque

[ISO/CEI Guide 73:2002]

3.15
traitement du risque
processus de sélection et de mise en œuvre des mesures visant à diminuer le risque

[ISO/CEI Guide 73:2002]

NOTE Dans la présente Norme internationale, le terme "contrôle" est utilisé comme synonyme de "mesure".

3.16
déclaration d'applicabilité (DdA)
déclaration documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées et applicables au SMSI d'un organisme

NOTE Les objectifs de sécurité et les mesures de sécurité proprement dites sont basés sur les résultats et les conclusions des processus de l'appréciation du risque et de traitement du risque, les exigences légales ou réglementaires, les obligations contractuelles et les exigences métier de l'organisme, relatives à la sécurité de l'information.

4 SMSI

4.1 Exigences générales

L'organisme doit établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI documenté dans le contexte des activités commerciales d'ensemble de l'organisme et des risques auxquels elles sont confrontées. Pour les besoins de la présente Norme internationale, le processus utilisé est basé sur le modèle PDCA illustré à la Figure 1.

4.2 Établissement et management du SMSI

4.2.1 Établissement du SMSI

L'organisme doit effectuer les tâches suivantes:

a) définir le domaine d'application et les limites du SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, de sa technologie, ainsi que des détails et de la justification de toutes exclusions du domaine d'application (voir 1.2);

b) définir une politique pour le SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, et de sa technologie, qui:

1) inclut un cadre pour fixer les objectifs et indiquer une orientation générale et des principes d'action concernant la sécurité de l'information;

2) tient compte des exigences liées à l'activité et des exigences légales ou réglementaires, ainsi que des obligations de sécurité contractuelles;

3) s'aligne sur le contexte de management du risque stratégique auquel est exposé l'organisme, dans lequel se dérouleront l'établissement et la mise à jour du SMSI;

4) établit les critères d'évaluation future du risque [voir 4.2.1c)];

5) a été approuvée par la direction.

NOTE Pour les besoins du présent document, les politiques relatives au SMSI sont considérées comme un surensemble de la politique relative à la sécurité de l'information. Ces politiques peuvent être décrites dans un seul document.

c) définir l'approche d'appréciation du risque de l'organisme:

1) identifier une méthodologie d'appréciation du risque adaptée au SMSI, ainsi qu'à la sécurité de l'information identifiée de l'organisme et aux exigences légales et réglementaires;

2) développer des critères d'acceptation des risques et identifier les niveaux de risque acceptables. [voir 5.1f)];

La méthodologie d'appréciation du risque choisie doit assurer que les appréciations du risque produisent des résultats comparables et reproductibles.

NOTE Il existe différentes méthodologies d'appréciation du risque. Des exemples de méthodologies d'appréciation du risque sont présentés dans l'ISO/CEI TR 13335-3, *Technologies de l'information — Lignes directrices pour la gestion de sécurité IT — Partie 3: Techniques pour la gestion de sécurité IT*.

d) identifier les risques:

1) identifier les actifs relevant du domaine d'application du SMSI, ainsi que leurs propriétaires[2)];

2) identifier les menaces auxquelles sont confrontés ces actifs;

3) identifier les vulnérabilités qui pourraient être exploitées par les menaces;

4) identifier les impacts que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs;

e) analyser et évaluer les risques:

1) évaluer l'impact sur l'activité de l'organisme qui pourrait découler d'une défaillance de la sécurité, en tenant compte des conséquences d'une perte de confidentialité, intégrité ou disponibilité des actifs;

2) évaluer la probabilité réaliste d'une défaillance de sécurité de cette nature au vu des menaces et des vulnérabilités prédominantes, des impacts associés à ces actifs et des mesures actuellement mises en œuvre;

3) estimer les niveaux des risques;

4) déterminer si les risques sont acceptables ou nécessitent un traitement, en utilisant les critères d'acceptation des risques établis en [4.2.1c)2)];

f) identifier et évaluer les choix de traitement des risques;

Les actions possibles comprennent:

1) l'application de mesures appropriées;

2) l'acceptation des risques en connaissance de cause et avec objectivité, dans la mesure où ils sont acceptables au regard des politiques de l'organisme et des critères d'acceptation des risques [voir 4.2.1c)2)];

3) l'évitement ou le refus des risques;

4) le transfert des risques liés à l'activité associés, à des tiers, par exemple assureurs, fournisseurs;

g) sélectionner les objectifs de sécurité et les mesures de sécurité proprement dites pour le traitement des risques.

Les objectifs de sécurité et les mesures de sécurité proprement dites doivent être sélectionnés et mis en œuvre pour répondre aux exigences identifiées par le processus d'appréciation du risque et de traitement du risque. Cette sélection doit tenir compte des critères d'acceptation des risques [voir 4.2.1c)] ainsi que des exigences légales, réglementaires et contractuelles.

---

2) Le terme "propriétaire" identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des actifs. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur l'actif.