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.

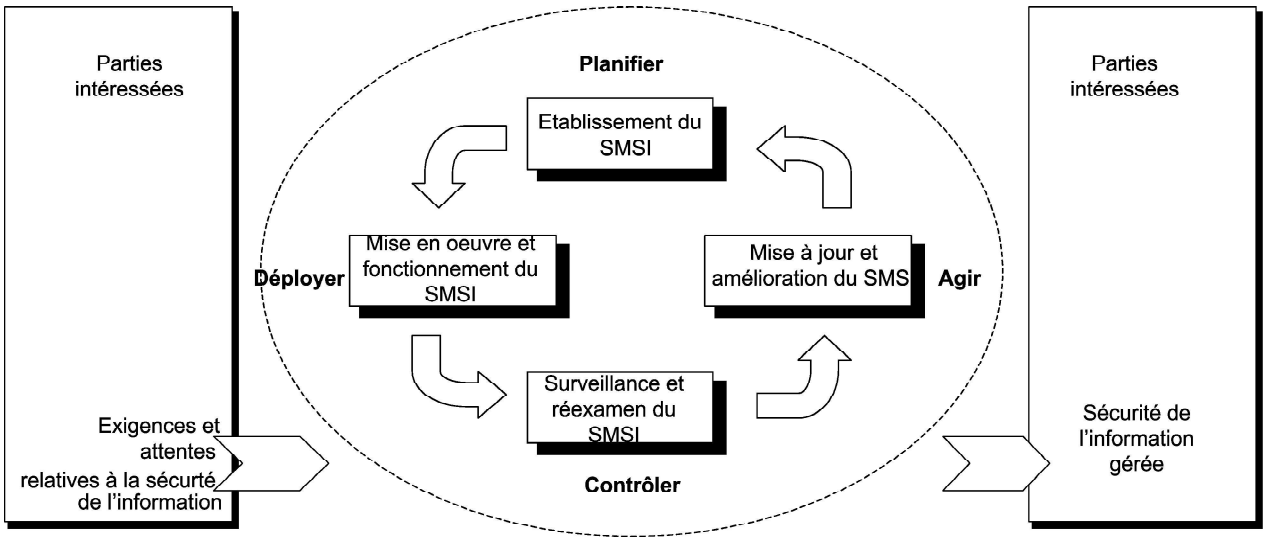

Figure 1 — Modèle PDCA appliqué aux processus SMSI

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.

Annexe C
(informative)

Correspondance entre l'ISO 9001:2000, l'ISO 14001:2004 et la présente Norme internationale

Le Tableau C.1 illustre la correspondance entre l'ISO 9001:2000, l'ISO 14001:2004 et la présente Norme internationale.

Tableau C.1 — Correspondance entre l'ISO 9001:2000, l'ISO 14001:2004 et la présente Norme internationale

La présente Norme internationale	ISO 9001:2000	ISO 14001:2004
Introduction	**0 Introduction**	**Introduction**
Généralités	0.1 Généralités	
Approche processus	0.2 Approche processus	
	0.3 Relation avec l'ISO 9004	
Compatibilité avec d'autres systèmes de management	0.4 Compatibilité avec d'autres systèmes de management	
1 Domaine d'application	**1 Domaine d'application**	**1 Domaine d'application**
1.1 Généralités	1.1 Généralités	
1.2 Application	1.2 Périmètre d'application	
2 Références normatives	**2 Référence normative**	**2 Référence normative**
3 Termes et définitions	**3 Termes et définitions**	**3 Termes et définitions**
4 SMSI	**4 Système de management de la qualité**	**4 Exigences du système de management environnemental**
4.1 Exigences générales	4.1 Exigences générales	4.1 Exigences générales
4.2 Établissement et management du SMSI		
4.2.1Établissement du SMSI		
4.2.2Mise en oeuvre et fonctionnement du SMSI		4.4 Mise en œuvre et fonctionnement
4.2.3Surveillance et réexamen du SMSI	8.2.3Surveillance et mesure des processus	4.5.1Surveillance et mesurage
	8.2.4Surveillance et mesure du produit	
4.2.4Mise à jour et amélioration du SMSI		
4.3 Exigences relatives à la documentation	4.2 Exigences relatives à la documentation	
4.3.1Généralités	4.2.1Généralités	
	4.2.2Manuel qualité	
4.3.2Maîtrise des documents	4.2.3Maîtrise des documents	4.4.5Maîtrise de la documentation
4.3.3Maîtrise des enregistrements	4.2.4Maîtrise des enregistrements	4.5.4Maîtrise des enregistrements

La présente Norme internationale	ISO 9001:2000	ISO 14001:2004
5 Responsabilité de la direction	**5 Responsabilité de la direction**	
5.1 Implication de la direction	5.1 Engagement de la direction	
	5.2 Écoute client	
	5.3 Politique qualité	4.2 Politique environnementale
	5.4 Planification	4.3 Planification
	5.5 Responsabilité, autorité et communication	
5.2 Management des ressources	**6 Management des ressources**	
5.2.1Mise à disposition des ressources	6.1 Mise à disposition des ressources	
	6.2 Ressources humaines	
5.2.2Formation, sensibilisation et compétence	6.2.2Compétence, sensibilisation et formation	4.4.2Compétence, formation et sensibilisation
	6.3 Infrastructures	
	6.4 Environnement de travail	
6 Audits internes du SMSI	8.2.2Audit interne	4.5.5 Audit interne
7 Revue de direction du SMSI	**5.6 Revue de direction**	**4.6 Revue de direction**
7.1 Généralités	5.6.1Généralités	
7.2 Éléments d'entrée du réexamen	5.6.2Éléments d'entrée de la revue	
7.3 Éléments de sortie du réexamen	5.6.3Éléments de sortie de la revue	
8 Amélioration du SMSI	**8.5 Amélioration**	
8.1 Amélioration continue	8.5.2Amélioration continue	
8.2 Action corrective	8.5.3Actions correctives	4.5.3Non-conformité, action corrective et action préventive
8.3 Action préventive	8.5.3Actions préventives	
Annexe A Objectifs de sécurité et mesures de sécurité		**Annexe A Lignes directrices pour l'utilisation de la présente Norme internationale**
Annexe B Les principes de l'OCDE et la présente Norme internationale		
Annexe C Correspondance entre l'ISO 9001:2000, l'ISO 14001:2004 et la présente Norme internationale	**Annexe A Correspondance entre l'ISO 9001:2000 et l'ISO 14001:1996**	**Annexe B Correspondance entre l'ISO 14001:2004 et l'ISO 9001:2000**