Norme Marocaine

NM ISO/CEI 27001

2009

(Indice de classement 00.5.701)

Technologies de l'information

Techniques de sécurité

Systèmes de gestion de la sécurité de l'information

Exigences

Norme Marocaine homologuée

Par arrêté du Ministre de l'Industrie, du Commerce et des Nouvelles Technologies N° du , publié au B.O. N° du

Correspondance

La présente norme reprend intégralement la norme ISO/CEI 27001/2005.

Modifications

Examinée et adoptée par le comité technique de normalisation des des systèmes de management
Editée et diffusée par le Service de Normalisation Industrielle Marocaine (SNIMA)

ICS :35.040

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.

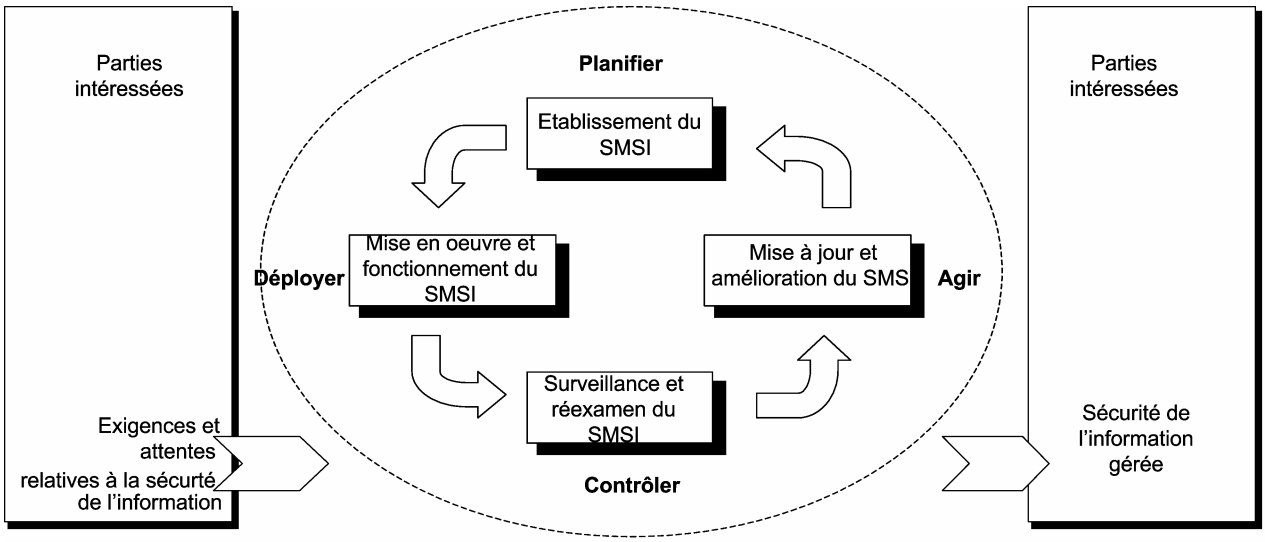

Figure 1 — Modèle PDCA appliqué aux processus SMSI

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.

Les objectifs de sécurité et les mesures de sécurité proprement dites définis à l'Annexe A doivent être sélectionnés comme partie intégrante de ce processus, dans la mesure où ils peuvent satisfaire à ces exigences.

Les objectifs de sécurité et les mesures de sécurité proprement dites énumérés à l'Annexe A ne sont pas exhaustifs et des objectifs de sécurité et des mesures de sécurité proprement dites additionnels peuvent également être sélectionnés.

NOTE L'Annexe A contient une liste complète d'objectifs de sécurité et des mesures de sécurité proprement dites qui se sont révélés communément appropriés aux organismes. Les utilisateurs de la présente Norme internationale doivent se reporter à l'Annexe A comme point de départ de sélection des mesures de sécurité, afin de s'assurer qu'aucune option importante de sécurité n'est négligée.

h) obtenir l'approbation par la direction des risques résiduels présentés;

i) obtenir l'autorisation de la direction pour mettre en œuvre et exploiter le SMSI;

j) préparer une DdA;

Une DdA doit être élaborée et inclure les informations suivantes:

1) les objectifs de sécurité et les mesures de sécurité proprement dites, sélectionnés en 4.2.1g) et les raisons pour lesquelles ils ont été sélectionnés;

2) les objectifs de sécurité et les mesures de sécurité proprement dites actuellement mis en œuvre [voir 4.2.1e)2)];

3) l'exclusion des objectifs de sécurité et des mesures de sécurité proprement dites spécifiés à l'Annexe A et la justification de leur exclusion.

NOTE La DdA fournit un résumé des décisions concernant le traitement du risque. La justification des exclusions prévoit une contre-vérification qui permet d'assurer qu'aucune mesure n'a été omise par inadvertance.

4.2.2 Mise en œuvre et fonctionnement du SMSI

L'organisme doit effectuer les tâches suivantes:

a) élaborer un plan de traitement du risque qui identifie les actions à engager, les ressources, les responsabilités et les priorités appropriées pour le management des risques liés à la sécurité de l'information (voir l'Article 5);

b) mettre en œuvre le plan de traitement du risque pour atteindre les objectifs de sécurité identifiés, ce plan prévoyant le mode de financement et l'affectation de rôles et de responsabilités;

c) mettre en œuvre les mesures de sécurité sélectionnées en 4.2.1g) afin de répondre aux objectifs de sécurité;

d) définir la méthode d'évaluation de l'efficacité des mesures ou groupes de mesures sélectionnés et spécifier comment ces évaluations doivent être utilisées pour évaluer l'efficacité des mesures, de manière à obtenir des résultats comparables et reproductibles [voir 4.2.3c)].

NOTE L'évaluation de l'efficacité des mesures permet aux dirigeants et au personnel de déterminer comment les mesures permettent pleinement d'atteindre les objectifs de sécurité prévus.

e) mettre en œuvre des programmes de formation et de sensibilisation (voir 5.2.2);

f) gérer les opérations du SMSI;

g) gérer les ressources consacrées au SMSI (voir 5.2);

h) mettre en œuvre les procédures et les autres mesures permettant de détecter rapidement et de répondre tout aussi rapidement aux incidents de sécurité (voir 4.2.3).

4.2.3 Surveillance et réexamen du SMSI

L'organisme doit effectuer les tâches suivantes:

a) exécuter les procédures de surveillance et de réexamen, ainsi que les autres mesures afin:

   1) de détecter rapidement les erreurs dans les résultats des traitements;

   2) d'identifier rapidement les failles et les incidents de sécurité;

   3) de permettre à la direction de déterminer si les activités de sécurité confiées au personnel ou mises en œuvre par les technologies de l'information sont exécutées comme prévu;

   4) de faciliter la détection des événements de sécurité, et par conséquent, de prévenir les incidents de sécurité par l'utilisation d'indicateurs;

   5) de déterminer si les actions entreprises pour résoudre une faille de sécurité se sont révélées efficaces.

b) réaliser des réexamens réguliers de l'efficacité du SMSI (y compris le respect de la politique et des objectifs du SMSI, et le réexamen des mesures de sécurité) en tenant compte des résultats des audits de sécurité, des incidents, des mesures de l'efficacité, des propositions et du retour d'information de toutes les parties intéressées;

c) d'évaluer l'efficacité des mesures afin de vérifier que les exigences de sécurité ont été satisfaites;

d) réexaminer les appréciations du risque à intervalles planifiés et réexaminer le niveau de risque résiduel et le niveau de risque acceptable identifié, compte tenu des changements apportés:

   1) à l'organisme;

   2) à la technologie;

   3) aux objectifs métiers et aux processus de l'organisme;

   4) aux menaces identifiées;

   5) à l'efficacité des mesures mises en œuvre;

   6) aux événements extérieurs, tels que les modifications apportées à la législation ou à la réglementation, aux obligations contractuelles et au climat social;

e) mener des audits internes du SMSI à intervalles fixés (voir Article 6);

NOTE Les audits internes, parfois appelés audits première partie, sont menés par, ou pour le compte de, l'organisme lui-même à des fins internes.

f) effectuer une revue de direction du SMSI de manière régulière afin de s'assurer du caractère toujours adéquat du domaine d'application du système et de l'identification des améliorations apportées au processus d'application du SMSI (voir 7.1);

g) mettre à jour les plans de sécurité afin de tenir compte des résultats des activités de surveillance et de réexamen;

h) consigner les actions et les événements qui pourraient avoir un impact sur l'efficacité ou les performances du SMSI (voir 4.3.3).

4.2.4 Mise à jour et amélioration du SMSI

L'organisme doit effectuer les tâches suivantes de manière régulière:

a) mettre en œuvre les améliorations identifiées du SMSI;

b) entreprendre les actions correctives et préventives appropriées conformément à 8.2 et 8.3. Appliquer les leçons tirées des expériences de sécurité des autres organismes, ainsi que de celles de l'organisme concerné;

c) informer toutes les parties prenantes des actions et améliorations, avec un niveau de détail approprié aux circonstances et, le cas échéant, convenir de la méthode à adopter;

d) s'assurer que les améliorations permettent d'atteindre leurs objectifs prévus.

4.3 Exigences relatives à la documentation

4.3.1 Généralités

La documentation doit inclure les enregistrements des décisions de gestion et assurer que les actions entreprises sont identifiables grâce aux décisions et aux politiques de la direction, et que les résultats consignés sont reproductibles.

Il est important de pouvoir démontrer la relation entre les mesures sélectionnées et les résultats du processus d'appréciation du risque et de traitement du risque, et par conséquent, la politique et les objectifs du SMSI.

La documentation du SMSI doit inclure:

a) les déclarations documentées de la politique et des objectifs du SMSI [voir 4.2.1b)];

b) le domaine d'application du SMSI [voir 4.2.1a)];

c) les procédures et les contrôles pour le SMSI;

d) une description de la méthodologie d'appréciation du risque [voir 4.2.1c)];

e) le rapport d'appréciation du risque [voir 4.2.1c) à 4.2.1g)];

f) le plan de traitement du risque [voir 4.2.2b)];

g) les procédures documentées dont a besoin l'organisme pour s'assurer de la planification, du fonctionnement et du contrôle effectifs de ses processus de sécurité de l'information et pour spécifier comment évaluer l'efficacité des mesures appliquées [voir 4.2.3c)];

h) les enregistrements exigés par la présente Norme internationale (voir 4.3.3);

i) la DdA.

NOTE 1 Lorsque le terme "procédure documentée" apparaît dans la présente Norme internationale, cela signifie que la procédure est établie, documentée, appliquée et mise à jour.

NOTE 2 L'étendue de la documentation du SMSI peut différer d'un organisme à l'autre en raison:

— de la taille de l'organisme et du type de ses activités;

— de la portée et de la complexité des exigences de sécurité, ainsi que du domaine d'application et de la complexité du système effectivement géré.

NOTE 3 Les documents et les enregistrements peuvent se présenter sous toute forme ou tout type de support.

4.3.2 Maîtrise des documents

Les documents requis pour le SMSI doivent être protégés et maîtrisés. Une procédure documentée doit être établie pour définir les actions à engager nécessaires pour:

a) approuver l'adéquation des documents avant diffusion;

b) réexaminer, mettre à jour si nécessaire et approuver de nouveau les documents;

c) assurer que les modifications et le statut de la version en vigueur des documents sont identifiés;

d) assurer la disponibilité sur les lieux d'utilisation des versions pertinentes des documents applicables;

e) assurer que les documents restent lisibles et facilement identifiables;

f) assurer la mise à disposition des documents aux personnes qui en ont besoin, ainsi que le transfert, le stockage et l'élimination finale desdits documents conformément aux procédures applicables à leur classification;

g) assurer que les documents d'origine extérieure sont identifiés;

h) assurer que la diffusion des documents est maîtrisée;

i) empêcher toute utilisation non intentionnelle de documents périmés;

j) les identifier de manière adéquate s'ils sont conservés dans un but quelconque.

4.3.3 Maîtrise des enregistrements

Les enregistrements doivent être établis et conservés pour apporter la preuve de la conformité aux exigences et du fonctionnement efficace du SMSI. Ils doivent être protégés et maîtrisés. Le SMSI doit tenir compte des exigences légales ou réglementaires et des obligations contractuelles. Les enregistrements doivent rester lisibles, faciles à identifier et accessibles. Les contrôles permettant d'assurer l'identification, le stockage, la protection, l'accessibilité, la durée de conservation et l'élimination des enregistrements doivent être documentés et mis en œuvre.

Les enregistrements des performances du processus tels que spécifiés en 4.2, ainsi que de toutes les occurrences des incidents de sécurité importants relatifs au SMSI, doivent être conservés.

EXEMPLE Le registre des visiteurs, les rapports d'audits et les formulaires complétés d'autorisation d'accès constituent des exemples d'enregistrements.

5 Responsabilité de la direction

5.1 Implication de la direction

La direction doit fournir la preuve de son implication dans l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI, par:

a) l'établissement d'une politique relative au SMSI;

b) l'assurance que des objectifs et des plans pour le SMSI sont établis;

c) la définition de rôles et de responsabilités pour la sécurité de l'information;

d) la sensibilisation de l'organisme à l'importance de satisfaire aux exigences relatives à la sécurité de l'information et de respecter la politique en matière de sécurité de l'information, à ses responsabilités au titre de la loi et à la nécessité d'une amélioration continue;

e) la fourniture de ressources suffisantes pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMSI (voir 5.2.1);

f) la détermination des critères d'acceptation des risques et des niveaux de risque acceptables;

g) l'assurance que des audits internes du SMSI sont menés (voir Article 6);

h) la réalisation de revues de direction du SMSI (voir Article 7).

5.2 Management des ressources

5.2.1 Mise à disposition des ressources

L'organisme doit déterminer et fournir les ressources nécessaires pour:

a) établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI;

b) assurer que les procédures de sécurité de l'information soutiennent les exigences métier;

c) identifier et traiter les exigences légales et réglementaires, ainsi que les obligations de sécurité contractuelles;

d) maintenir une sécurité adéquate par une application correcte de toutes les mesures mises en œuvre;

e) effectuer des réexamens si nécessaire, et réagir de manière appropriée aux résultats de ces réexamens;

f) améliorer, le cas échéant, l'efficacité du SMSI.

5.2.2 Formation, sensibilisation et compétence

L'organisme doit s'assurer que le personnel à qui a été affecté les responsabilités définies dans le SMSI, a les compétences nécessaires pour exécuter les tâches requises, en:

a) déterminant les compétences nécessaires pour le personnel effectuant un travail ayant une incidence sur le SMSI;

b) fournissant la formation ou en entreprenant d'autres actions (par exemple emploi d'un personnel compétent) pour satisfaire ces besoins;

c) évaluant l'efficacité des actions entreprises;

d) conservant les enregistrements concernant la formation initiale et professionnelle, le savoir-faire, l'expérience et les qualifications (voir 4.3.3).

L'organisme doit également s'assurer que tout le personnel approprié a conscience de la pertinence et de l'importance de ses activités liées à la sécurité de l'information et de la façon dont ces dernières contribuent à l'atteinte des objectifs du SMSI.

6 Audits internes du SMSI

L'organisme doit mener des audits internes du SMSI à intervalles planifiés pour déterminer si les objectifs de sécurité, les mesures, les processus et les procédures de son SMSI:

a) sont conformes aux exigences de la présente Norme internationale et à la législation ou aux règlements pertinents;

b) sont conformes aux exigences de sécurité de l'information identifiées;

c) sont mis en œuvre et tenus à jour de manière efficace;

d) sont exécutés tel que prévu.

Un programme d'audit doit être planifié en tenant compte de l'état et de l'importance des processus et des domaines à auditer, ainsi que des résultats des audits précédents. Les critères, le champ, la fréquence et les méthodes d'audit doivent être définis. Le choix des auditeurs et la réalisation des audits doivent assurer l'objectivité et l'impartialité du processus d'audit. Les auditeurs ne doivent pas auditer leur propre travail.

Les responsabilités et les exigences pour planifier, mener les audits, rendre compte des résultats et conserver des enregistrements (voir 4.3.3) doivent être définies dans une procédure documentée.

L'encadrement responsable du domaine audité doit assurer que des actions sont entreprises sans délai indu pour éliminer les non-conformités détectées et leurs causes. Les activités de suivi doivent inclure la vérification des actions entreprises et le compte-rendu des résultats de cette vérification (voir Article 8).

NOTE L'ISO19011:2002, *Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*, peut également fournir des directives utiles pour mener les audits internes du SMSI.

7 Revue de direction du SMSI

7.1 Généralités

La direction doit, à intervalles planifiés (au moins une fois par an), procéder au réexamen du SMSI de l'organisme pour assurer qu'il demeure pertinent, adéquat et efficace. Ce réexamen doit comprendre l'évaluation des opportunités d'amélioration et du besoin de modifier le SMSI, y compris la politique et les objectifs de sécurité de l'information. Les résultats des réexamens doivent être clairement documentés et les enregistrements doivent être conservés (voir 4.3.3).

7.2 Éléments d'entrée du réexamen

Les éléments d'entrée d'une revue de direction doivent comprendre des informations sur:

a) les résultats des audits et des réexamens du SMSI;

b) les retours d'information des parties intéressées;

c) les techniques, produits ou procédures que pourrait utiliser l'organisme pour améliorer les performances et l'efficacité du SMSI;

d) l'état des actions préventives et correctives;

e) les vulnérabilités ou les menaces qui n'ont pas été traitées de manière adéquate dans l'appréciation du risque précédente;

f) les résultats des mesures de l'efficacité;

g) les actions de suivi issues des revues de direction précédentes;

h) tous changements pouvant affecter le SMSI;

i) les recommandations d'amélioration.

7.3 Éléments de sortie du réexamen

Les éléments de sortie de la revue de direction doivent comporter les décisions et actions relatives aux informations suivantes:

a) l'amélioration de l'efficacité du SMSI;

b) la mise à jour du plan d'appréciation du risque et de traitement du risque;

c) la modification des procédures et mesures qui affectent la sécurité de l'information, si nécessaire, pour répondre aux événements intérieurs ou extérieurs qui peuvent exercer une influence sur le SMSI, y compris les modifications:

   1) des exigences métier;

   2) des exigences de sécurité;

   3) des processus métier affectant les exigences métier existantes;

   4) des exigences légales ou réglementaires;

   5) des obligations contractuelles;

   6) des niveaux de risque et/ou des critères d'acceptation des risques.

d) les besoins en ressources;

e) l'amélioration de la méthode d'évaluation de l'efficacité des mesures.

8 Amélioration du SMSI

8.1 Amélioration continue

L'organisme doit améliorer en permanence l'efficacité du SMSI en utilisant la politique en matière de sécurité de l'information, la réalisation des objectifs en termes de sécurité de l'information, les résultats d'audit, l'analyse des événements surveillés, les actions correctives et préventives et la revue de direction (voir Article 7).

8.2 Action corrective

L'organisme doit mener des actions pour éliminer les causes de non-conformités avec les exigences du SMSI, afin d'éviter qu'elles ne se reproduisent. La procédure documentée pour l'action corrective doit définir les exigences relatives à:

a) l'identification des non-conformités;

b) la détermination des causes des non-conformités;

c) l'évaluation du besoin d'entreprendre des actions pour que les non-conformités ne se reproduisent pas;

d) la détermination et la mise en œuvre de l'action corrective requise;

e) la consignation des résultats de l'action entreprise (voir 4.3.3);

f) le réexamen de l'action corrective entreprise.

8.3 Action préventive

L'organisme doit déterminer l'action permettant d'éliminer la cause des non-conformités potentielles avec les exigences du SMSI, afin d'éviter qu'elles ne surviennent. Les actions préventives doivent être adaptées aux effets des problèmes potentiels. La procédure documentée pour l'action préventive doit définir les exigences relatives à:

a) l'identification des non-conformités potentielles et de leurs causes;

b) l'évaluation du besoin d'entreprendre des actions pour éviter l'apparition de non-conformités;

c) la détermination et la mise en œuvre de l'action préventive requise;

d) la consignation des résultats de l'action entreprise (voir 4.3.3);

e) le réexamen de l'action préventive entreprise.

L'organisme doit identifier les risques modifiés et les exigences relatives aux actions préventives, en concentrant son attention sur les risques soumis à une modification importante.

La priorité des actions préventives doit être déterminée sur la base des résultats de l'appréciation du risque.

NOTE L'action visant à prévenir les non-conformités est souvent plus rentable que l'action corrective.

Annexe A
(normative)

Objectifs de sécurité et mesures de sécurité

Les objectifs de sécurité et les mesures de sécurité énumérés dans le Tableau A.1 proviennent directement et sont alignés sur les objectifs de sécurité et les mesures de sécurité énumérés dans l'ISO/CEI 17799:2005, Articles 5 à 15. Les listes figurant dans ces tableaux ne sont pas exhaustives et un organisme peut considérer nécessaires des objectifs de sécurité et des mesures de sécurité additionnels. Les objectifs de sécurité et les mesures de sécurité mentionnés dans ces tableaux doivent être sélectionnés comme partie intégrante du processus d'application du SMSI spécifié en 4.2.1.

Les Articles 5 à 15 de l'ISO/CEI 17799:2005 fournissent des recommandations de mise en œuvre et des lignes directrices afférentes aux meilleures pratiques, venant à l'appui des mesures spécifiées aux paragraphes A.5 à A.15.

Tableau A.1 — Objectifs de sécurité et mesures de sécurité

A.5 Politique de sécurité		
A.5.1 Politique de sécurité de l'information *Objectif:* Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.1.1	Document de politique de sécurité de l'information	*Mesure* Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.
A.5.1.2	Réexamen de la politique de sécurité de l'information	*Mesure* Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, la politique doit être réexaminée à intervalles fixés préalablement ou en cas de changements majeurs.
A.6 Organisation de la sécurité de l'information		
A.6.1 Organisation interne *Objectif:* Gérer la sécurité de l'information au sein de l'organisme.		
A.6.1.1	Implication de la direction vis-à-vis de la sécurité de l'information	*Mesure* La direction doit soutenir activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.
A.6.1.2	Coordination de la sécurité de l'information	*Mesure* Les activités relatives à la sécurité de l'information doivent être coordonnées par des intervenants ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme.
A.6.1.3	Attribution des responsabilités en matière de sécurité de l'information	*Mesure* Toutes les responsabilités en matière de sécurité de l'information doivent être définies clairement.
A.6.1.4	Système d'autorisation concernant les moyens de traitement de l'information	*Mesure* Un système de gestion des autorisations doit être défini et mis en œuvre pour chaque nouveau moyen de traitement de l'information.

A.6.1.5	Engagements de confidentialité	*Mesure* Les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme, doivent être identifiées et réexaminées régulièrement.
A.6.1.6	Relations avec les autorités	*Mesure* Des relations appropriées doivent être mises en place avec les autorités compétentes.
A.6.1.7	Relations avec des groupes de spécialistes	*Mesure* Des contacts appropriés doivent être entretenus avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.
A.6.1.8	Réexamen indépendant de la sécurité de l'information	*Mesure* Des réexamens réguliers et indépendants de l'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (c'est-à-dire le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectués; de tels réexamens sont également nécessaires lorsque des changements importants sont intervenus dans la mise en œuvre de la sécurité.
A.6.2 Tiers *Objectif:* Assurer la sécurité de l'information et des moyens de traitement de l'information appartenant à l'organisme et consultés, traités, communiqués ou gérés par des tiers.		
A.6.2.1	Identification des risques provenant des tiers	*Mesure* Les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers doivent être identifiés, et des mesures appropriées doivent être mises en œuvre avant d'accorder des accès.
A.6.2.2	La sécurité et les clients	*Mesure* Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux actifs de l'organisme.
A.6.2.3	La sécurité dans les accords conclus avec des tiers	*Mesure* Les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, doivent couvrir l'ensemble des exigences applicables en matière de sécurité.

A.7 Gestion des actifs		
A.7.1 Responsabilités relatives aux actifs		
Objectif: Mettre en place et maintenir une protection appropriée des actifs de l'organisme.		
A.7.1.1	Inventaire des actifs	*Mesure* Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré.
A.7.1.2	Propriété des actifs	*Mesure* La propriété de chaque information et des moyens de traitement de l'information doit être 'attribuée[3)]' à une partie définie de l'organisme.
A.7.1.3	Utilisation correcte des actifs	*Mesure* Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.
A.7.2 Classification des informations		
Objectif: Garantir un niveau de protection approprié aux informations.		
A.7.2.1	Lignes directrices pour la classification	*Mesure* Les informations doivent être classées en termes de valeur, d'exigences légales, de sensibilité et de criticité.
A.7.2.2	Marquage et manipulation de l'information	*Mesure* Un ensemble approprié de procédures pour le marquage et la manipulation de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisme.

3) Explication: 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.

A.8 Sécurité liée aux ressources humaines		
A.8.1 Avant le recrutement[4)] *Objectif:* Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées et réduire le risque de vol, de fraude ou de mauvais usage des équipements.		
A.8.1.1	Rôles et responsabilités	*Mesure* Les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers doivent être définis et documentés conformément à la politique de sécurité de l'information de l'organisme.
A.8.1.2	Sélection	*Mesure* Qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, les vérifications des informations concernant tous les candidats doivent être réalisées conformément aux lois, aux règlements et à l'étique et doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.
A.8.1.3	Conditions d'embauche	*Mesure* Dans le cadre de leurs obligations contractuelles, les salariés, contractants et utilisateurs tiers doivent se mettre d'accord sur les modalités du contrat d'embauche les liant et le signer. Ce contrat doit définir leurs responsabilités et celles de l'organisme quant à la sécurité de l'information.
A.8.2 Pendant la durée du contrat *Objectif:* Veiller à ce que tous les salariés, contractants et utilisateurs tiers soient conscients des menaces pesant sur la sécurité de l'information, de leurs responsabilités financières ou autres, et disposent des éléments requis pour prendre en charge la politique de sécurité de l'organisme dans le cadre de leur activité normale et réduire le risque d'erreur humaine.		
A.8.2.1	Responsabilités de la direction	*Mesure* La direction doit demander aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.
A.8.2.2	Sensibilisation, qualification et formations en matière de sécurité de l'information	*Mesure* L'ensemble des salariés d'un organisme et, le cas échant, les contractants et utilisateurs tiers doivent suivre une formation adaptée sur la sensibilisation et doivent recevoir régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.
A.8.2.3	Processus disciplinaire	*Mesure* Un processus disciplinaire formel doit être élaboré pour les salariés ayant enfreint les règles de sécurité.

4) Explication: Le terme "recrutement" défini ici couvre toutes les différentes situations suivantes: recrutement de personnes (durée provisoire ou plus longue durée), affectation de domaines d'activité, modification de domaines d'activité, cession de contrats et résiliation de l'un de ces contrats.

A.8.3 Fin ou modification du contrat		
Objectif: Veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie.		
A.8.3.1	Responsabilités en fin de contrat	*Mesure* Les responsabilités relatives aux fins ou aux modifications de contrats doivent être clairement définies et attribuées.
A.8.3.2	Restitution des actifs	*Mesure* Tous les salariés, contractants et utilisateurs tiers doivent restituer la totalité des actifs de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.
A.8.3.3	Retrait des droits d'accès	*Mesure* Les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.
A.9 Sécurité physique et environnementale		
A.9.1 Zones sécurisées		
Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.		
A.9.1.1	Périmètre de sécurité physique	*Mesure* Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).
A.9.1.2	Contrôles physiques des accès	*Mesure* Les zones sécurisées doivent être protégées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité est admis.
A.9.1.3	Sécurisation des bureaux, des salles et des équipements	*Mesure* Des mesures de sécurité physique doivent être conçues et appliquées pour les bureaux, les salles et les équipements.
A.9.1.4	Protection contre les menaces extérieures et environnementales	*Mesure* Des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme, doivent être conçues et appliquées.
A.9.1.5	Travail dans les zones sécurisées	*Mesure* Des mesures de protection physique et des directives pour le travail en zone sécurisée doivent être conçues et appliquées.
A.9.1.6	Zones d'accès public, de livraison et de chargement	*Mesure* Les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux doivent être contrôlés. Les points d'accès doivent également, si possible, être isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

A.9.2 Sécurité du matériel		
Objectif: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisme.		
A.9.2.1	Choix de l'emplacement et protection du matériel	*Mesure* Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.
A.9.2.2	Services généraux	*Mesure* Le matériel doit être protégé des coupures de courant et autres perturbations dues à une défaillance des services généraux.
A.9.2.3	Sécurité du câblage	*Mesure* Les câbles électriques ou de télécommunications transportant des données doivent être protégés contre toute interception d'information ou dommage.
A.9.2.4	Maintenance du matériel	*Mesure* Le matériel doit être entretenu correctement pour garantir sa disponibilité permanente et son intégrité.
A.9.2.5	Sécurité du matériel hors des locaux	*Mesure* La sécurité doit être appliquée au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.
A.9.2.6	Mise au rebut ou recyclage sécurisé(e) du matériel	*Mesure* Tout le matériel contenant des supports de stockage doit être vérifié pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut.
A.9.2.7	Sortie d'un actif	*Mesure* Un matériel, des informations ou des logiciels ne doivent pas être sortis des locaux de l'organisme sans autorisation préalable.
A.10 Gestion de l'exploitation et des télécommunications		
A.10.1 Procédures et responsabilités liées à l'exploitation		
Objectif: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.		
A.10.1.1	Procédures d'exploitation documentées	*Mesure* Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.
A.10.1.2	Management des modifications	*Mesure* Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés.
A.10.1.3	Séparation des tâches	*Mesure* Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme.
A.10.1.4	Séparation des équipements de développement, d'essai et d'exploitation	*Mesure* Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.

A.10.2 Gestion de la prestation de service conclus avec un tiers		
Objectif: Mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme aux accords de prestation de service conclus avec un tiers.		
A.10.2.1	Prestation de service	*Mesure* Il doit être assuré que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers.
A.10.2.2	Surveillance et examen des services tiers	*Mesure* Les services, rapports et enregistrements fournis par les tiers doivent être régulièrement contrôlés et réexaminés, et des audits doivent être régulièrement réalisés.
A.10.2.3	Gestion des modifications dans les services tiers	*Mesure* Les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.
A.10.3 Planification et acceptation du système		
Objectif: Réduire le plus possible le risque de pannes du système.		
A.10.3.1	Dimensionnement	*Mesure* L'utilisation des ressources doit être surveillée et ajustée au plus près, et des projections doivent être faites sur les dimensionnements futurs pour assurer les performances requises par le système.
A.10.3.2	Acceptation du système	*Mesure* Les critères d'acceptation doivent être fixés pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation.
A.10.4 Protection contre les codes malveillant et mobile		
Objectif: Protéger l'intégrité des logiciels et de l'information.		
A.10.4.1	Mesures contre les codes malveillants	*Mesure* Des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre.
A.10.4.2	Mesures contre le code mobile	*Mesure* Lorsque l'utilisation de code mobile est autorisée, la configuration doit garantir que le code mobile fonctionne selon une politique de sécurité clairement définie et tout code mobile non autorisé doit être bloqué.
A.10.5 Sauvegarde		
Objectif: Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.		
A.10.5.1	Sauvegarde des informations	*Mesure* Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

A.10.6 Gestion de la sécurité des réseaux		
Objectif: Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle elles s'appuient.		
A.10.6.1	Mesures sur les réseaux	*Mesure* Les réseaux doivent être gérés et contrôlés de manière adéquate pour qu'ils soient protégés des menaces et pour maintenir la sécurité des systèmes et des applications utilisant le réseau, notamment les informations en transit.
A.10.6.2	Sécurité des services réseau	*Mesure* Pour tous les services réseau, les fonctions réseau, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.
A.10.7 Manipulation des supports		
Objectif: Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) d'actifs et l'interruption des activités de l'organisme.		
A.10.7.1	Gestion des supports amovibles	*Mesure* Des procédures doivent être mises en place pour la gestion des supports amovibles.
A.10.7.2	Mise au rebut des supports	*Mesure* Les supports qui ne servent plus doivent être mis au rebut de façon sûre, en suivant des procédures formelles.
A.10.7.3	Procédures de manipulation des informations	*Mesure* Des procédures de manipulation et de stockage des informations doivent être établies pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage.
A.10.7.4	Sécurité de la documentation système	*Mesure* La documentation système doit être protégée contre les accès non autorisés.

A.10.8 Echange des informations		
Objectif: Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.		
A.10.8.1	Politiques et procédures d'échange des informations	*Mesure* Des politiques, procédures et mesures d'échange formelles doivent être mises en place pour protéger les échanges d'informations liées à tous types d'équipements de télécommunication.
A.10.8.2	Accords d'échange	*Mesure* Des accords doivent être conclus pour l'échange d'informations et de logiciels entre l'organisme et la partie externe.
A.10.8.3	Supports physiques en transit	*Mesure* Les supports contenant des informations doivent être protégés contre les accès non autorisés, le mauvais usage ou l'altération lors du transport hors des limites physiques de l'organisme.
A.10.8.4	Messagerie électronique	*Mesure* Les informations liées à la messagerie électronique doivent être protégées de manière adéquate.
A.10.8.5	Systèmes d'information d'entreprise	*Mesure* Des politiques et procédures doivent être élaborées et mises en œuvre pour protéger l'information liée à l'interconnexion de systèmes d'informations d'entreprise.
A.10.9 Services de commerce électronique		
Objectif: Assurer la sécurité des services de commerce électronique, ainsi que leur utilisation sécurisée.		
A.10.9.1	Commerce électronique	*Mesure* Les informations liées au commerce électronique transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les litiges sur les contrats et la divulgation et la modification non autorisées.
A.10.9.2	Transactions en ligne	*Mesure* Les informations liées aux transactions en ligne doivent être protégées pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission.
A.10.9.3	Informations à disposition du public	*Mesure* L'intégrité des informations mises à disposition sur un système accessible au public doit être protégée pour empêcher toute modification non autorisée.
A.10.10 Surveillance		
Objectif: Détecter les traitements non autorisés de l'information.		
A.10.10.1	Journaux d'audit	*Mesure* Les journaux d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès.
A.10.10.2	Surveillance de l'exploitation du système	*Mesure* Des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information doivent être établies et les résultats des activités de surveillance doivent être réexaminés périodiquement.

A.10.10.3	Protection des informations journalisées	*Mesure* Les équipements de journalisation et les informations journalisées doivent être protégés contre le sabotage et les accès non autorisés.
A.10.10.4	Journal administrateur et journal des opérations	*Mesure* Les activités de l'administrateur système et de l'opérateur système doivent être journalisées.
A.10.10.5	Rapports d'anomalies	*Mesure* Les éventuels défauts doivent être journalisés et analysés et les mesures appropriées doivent être prises.
A.10.10.6	Synchronisation des horloges	*Mesure* Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de temps précise et préalablement définie.
A.11 Contrôle d'accès		
A.11.1 Exigences métier relatives au contrôle d'accès *Objectif:* Maîtriser l'accès à l'information.		
A.11.1.1	Politique de contrôle d'accès	*Mesure* Une politique de contrôle d'accès doit être établie, documentée et réexaminée sur la base des exigences métier et de sécurité.
A.11.2 Gestion des accès des utilisateurs *Objectif:* Contrôler l'accès des utilisateurs autorisés et empêcher les accès non autorisés aux systèmes d'information.		
A.11.2.1	Enregistrement des utilisateurs	*Mesure* Une procédure formelle d'inscription et désincription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie.
A.11.2.2	Gestion des privilèges	*Mesure* L'attribution et l'utilisation des privilèges doivent être restreintes et contrôlées.
A.11.2.3	Gestion du mot de passe utilisateur	*Mesure* L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.
A.11.2.4	Réexamen des droits d'accès utilisateurs	*Mesure* La direction doit réexaminer les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.

A.11.3 Responsabilités de l'utilisateurs		
Objectif: Empêcher l'accès d'utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information.		
A.11.3.1	Utilisation du mot de passe	*Mesure* Il doit être demandé aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.
A.11.3.2	Matériel utilisateur laissé sans surveillance	*Mesure* Les utilisateurs doivent s'assurer que tout matériel laissé sans surveillance est doté d'une protection appropriée.
A.11.3.3	Politique du bureau propre et de l'écran vide	*Mesure* Une politique du bureau propre doit être adoptée pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide doit également être adoptée pour les moyens de traitement de l'information.
A.11.4 Contrôle d'accès réseau		
Objectif: Empêcher les accès non autorisés aux services disponibles sur le réseau.		
A.11.4.1	Politique relative à l'utilisation des services en réseau	*Mesure* Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.
A.11.4.2	Authentification de l'utilisateur pour les connexions externes	*Mesure* Des méthodes d'authentification appropriées doivent être utilisées pour contrôler l'accès des utilisateurs distants.
A.11.4.3	Identification des matériels en réseaux	*Mesure* L'identification automatique de matériels doit être considérée comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques.
A.11.4.4	Protection des ports de diagnostic et de configuration à distance	*Mesure* L'accès physique et logique aux ports de diagnostic et de configuration à distance doit être contrôlé.
A.11.4.5	Cloisonnement des réseaux	*Mesure* Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être séparés sur le réseau.
A.11.4.6	Mesure relative à la connexion réseau	*Mesure* Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, la capacité de connexion réseau des utilisateurs doit être restreinte, conformément à la politique de contrôle d'accès et aux exigences relatives aux applications métier (voir 11.1)
A.11.4.7	Contrôle du routage réseau	*Mesure* Des mesures du routage des réseaux doivent être mises en œuvre afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications métier.

A.11.5 Contrôle d'accès au système d'exploitation		
Objectif: Empêcher les accès non autorisés aux systèmes d'exploitation.		
A.11.5.1	Ouverture de sessions sécurisées	*Mesure* L'accès aux systèmes d'exploitation doit être soumis à une procédure sécurisée d'ouverture de session.
A.11.5.2	Identification et authentification de l'utilisateur	*Mesure* Un identifiant unique et exclusif doit être attribué à chaque utilisateur et une technique d'authentification doit être choisie, permettant de vérifier l'identité déclarée par l'utilisateur.
A.11.5.3	Système de gestion des mots de passe	*Mesure* Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent fournir des mots de passe de qualité.
A.11.5.4	Emploi des utilitaires système	*Mesure* L'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application doit être limité et contrôlé étroitement.
A.11.5.5	Déconnexion automatique des sessions inactives	*Mesure* Les sessions inactives doivent être déconnectées après une période d'inactivité définie.
A.11.5.6	Limitation du temps de connexion	*Mesure* Les temps de connexion doivent être restreints afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.
A.11.6 Contrôle d'accès aux applications et à l'information		
Objectif: Empêcher les accès non autorisés aux informations stockées dans les applications.		
A.11.6.1	Restriction d'accès à l'information	*Mesure* Pour les utilisateurs et le personnel chargé de l'assistance technique, l'accès aux informations et aux fonctions applicatives doit être restreint conformément à la politique de contrôle d'accès.
A.11.6.2	Isolement des systèmes sensibles	*Mesure* Les systèmes sensibles doivent disposer d'un environnement informatique dédié (isolé).
A.11.7 Informatique mobile et télétravail		
Objectif: Garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles et d'équipements de télétravail.		
A.11.7.1	Informatique et communications mobiles	*Mesure* Une procédure formelle et des mesures de sécurité appropriées doivent être mises en place pour assurer une protection contre le risque lié à l'utilisation d'appareils informatiques et de communication mobiles.
A.11.7.2	Télétravail	*Mesure* Une politique, des procédures et des programmes opérationnels spécifiques au télétravail doivent être élaborés et mis en œuvre.

A.12 Acquisition, développement et maintenance des systèmes d'information		
A.12.1 Exigences de sécurité applicables aux systèmes d'information		
Objectif: Veiller à ce que la sécurité fasse partie intégrante des systèmes d'information.		
A.12.1.1	Analyse et spécification des exigences de sécurité	*Mesure* Les exigences métier relatives aux nouveaux systèmes d'information ou les améliorations apportées aux systèmes d'information existants doivent spécifier les exigences de sécurité.
A.12.2 Bon fonctionnement des applications		
Objectif: Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications.		
A.12.2.1	Validation des données en entrée	*Mesure* Les données entrées dans les applications doivent être validées afin de vérifier si elles sont correctes et appropriées.
A.12.2.2	Mesure relative au traitement interne	*Mesure* Des contrôles de validation doivent être inclus dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés.
A.12.2.3	Intégrité des messages	*Mesure* Les exigences permettant d'assurer l'authentification et la protection de l'intégrité des messages dans les applications doivent être identifiées, et des mesures appropriées doivent être identifiées et mises en œuvre.
A.12.2.4	Validation des données en sortie	*Mesure* Les données de sortie d'une application doivent être validées pour assurer que le traitement des informations stockées est correct et adapté aux circonstances.
A.12.3 Mesures cryptographiques		
Objectif: Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.		
A.12.3.1	Politique d'utilisation des mesures cryptographiques	*Mesure* Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.
A.12.3.2	Gestion des clés	*Mesure* Une procédure de gestion des clés doit favoriser l'utilisation par l'organisme de techniques cryptographiques.
A.12.4 Sécurité des fichiers système		
Objectif: Garantir la sécurité des fichiers système.		
A.12.4.1	Mesure relative aux logiciels en exploitation	*Mesure* Des procédures doivent être mises en place pour contrôler l'installation du logiciel sur les systèmes en exploitation.
A.12.4.2	Protection des données système d'essai	*Mesure* Les données d'essai doivent être sélectionnées avec soin, protégées et contrôlées.
A.12.4.3	Contrôle d'accès au code source du programme	*Mesure* L'accès au code source du programme doit être restreint.

A.12.5 Sécurité en matière de développement et d'assistance technique		
Objectif: Garantir la sécurité du logiciel et des informations d'application.		
A.12.5.1	Procédures de contrôle des modifications	*Mesure* La mise en œuvre des modifications doit être contrôlée par le biais de procédures formelles.
A.12.5.2	Réexamen technique des applications après modification du système d'exploitation	*Mesure* Lorsque des modifications sont apportées aux systèmes d'exploitation, les applications critiques métier doivent être réexaminées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.
A.12.5.3	Restrictions relatives à la modification des progiciels	*Mesure* La modification des progiciels ne doit pas être encouragée, et doit être limitée aux changements nécessaires. Un contrôle strict doit également être exercé sur ces modifications.
A.12.5.4	Fuite d'informations	*Mesure* Toute possibilité de fuite d'informations doit être empêchée.
A.12.5.5	Externalisation du développement logiciel	*Mesure* Le développement logiciel externalisé doit être encadré et contrôlé par l'organisme.
A.12.6 Gestion des vulnérabilités techniques		
Objectif: Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.		
A.12.6.1	Mesure relative aux vulnérabilités techniques	*Mesure* Toute information concernant toute vulnérabilité technique des systèmes d'information en exploitation doit être obtenue à temps, l'exposition de l'organisme aux dites vulnérabilités doit être évaluée et les actions appropriées doivent être entreprises pour traiter le risque associé.
A.13 Gestion des incidents liés à la sécurité de l'information		
A.13.1 Remontée des événements et des failles liés à la sécurité de l'information		
Objectif: Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permet la mise en œuvre d'une action corrective, dans les meilleurs délais.		
A.13.1.1	Remontée des événements liés à la sécurité de l'information	*Mesure* Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées.
A.13.1.2	Remontée des failles de sécurité	*Mesure* Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

A.13.2 Gestion des incidents liés à la sécurité de l'information et des améliorations		
Objectif: Garantir la mise en place d'une approche cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information.		
A.13.2.1	Responsabilités et procédures	*Mesure* Des responsabilités et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.
A.13.2.2	Exploitation des incidents liés à la sécurité de l'information déjà survenus	*Mesure* Des mécanismes doivent être mis en place, permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés.
A.13.2.3	Collecte de preuves	*Mesure* Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de preuve doivent être recueillis, conservés et présentés conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).
A.14 Gestion de la continuité de l'activité		
A.14.1 Gestion de la continuité de l'activité d'un point de vue aspects de la sécurité de l'information		
Objectif: Empêcher les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les défaillances majeures des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.		
A.14.1.1	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité	*Mesure* Un processus de continuité de l'activité dans l'ensemble de l'organisme doit être élaboré et géré, qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.
A.14.1.2	Continuité de l'activité et appréciation du risque	*Mesure* Les événements pouvant être à l'origine d'interruptions des processus métier doivent être identifiés, tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.
A.14.1.3	Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	*Mesure* Des plans doivent être élaborés et mis en œuvre pour maintenir ou restaurer l'exploitation et assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.
A.14.1.4	Cadre de la planification de la continuité de l'activité	*Mesure* Un cadre unique pour les plans de continuité de l'activité doit être géré afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance.
A.14.1.5	Mise à l'essai, gestion et réévaluation constante des plans de continuité de l'activité	*Mesure* Les plans de continuité de l'activité doivent être testés et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces.

A.15 Conformité		
A.15.1 Conformité aux exigences légales		
Objectif: Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles et des exigences de sécurité.		
A.15.1.1	Identification de la législation en vigueur	*Mesure* Pour chaque système d'information et pour l'organisme, toutes les exigences légales, réglementaires et contractuelles en vigueur doivent être définies, documentées et mises à jour, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.
A.15.1.2	Droits de propriété intellectuelle (DPI)	*Mesure* Des procédures appropriées doivent être mises en œuvre, visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.
A.15.1.3	Protection des enregistrements de l'organisme	*Mesure* Les enregistrements importants doivent être protégés contre la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier.
A.15.1.4	Protection des données et confidentialité des informations relatives à la vie privée	*Mesure* La protection et la confidentialité des données doivent être garanties, telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.
A.15.1.5	Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information	*Mesure* Les utilisateurs doivent être dissuadés de toute utilisation de moyens de traitement de l'information à des fins illégales.
A.15.1.6	Réglementation relative aux mesures cryptographiques	*Mesure* Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables.
A.15.2 Conformité avec les politiques et normes de sécurité et conformité technique		
Objectif: S'assurer de la conformité des systèmes avec les politiques et normes de sécurité de l'organisme.		
A.15.2.1	Conformité avec les politiques et les normes de sécurité	*Mesure* Les responsables doivent s'assurer de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.
A.15.2.2	Vérification de la conformité technique	*Mesure* La conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité doit être vérifiée régulièrement.

A.15.3 Prises en compte de l'audit du système d'information *Objectif:* Optimiser l'efficacité et réduire le plus possible l'interférence avec le/du processus d'audit du système d'information.		
A.15.3.1	Contrôles de l'audit du système d'information	*Mesure* Les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation doivent être planifiées de manière précise et doivent être le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier.
A.15.3.2	Protection des outils d'audit du système d'information	*Mesure* L'accès aux outils d'audit du système d'information doit être protégé afin d'empêcher tous mauvais usage ou compromission éventuels.

Annexe B
(informative)

Les principes de l'OCDE et la présente Norme internationale

Les principes donnés dans les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information s'appliquent à tous les niveaux, politique et opérationnel, qui régissent la sécurité des systèmes et réseaux d'information. La présente Norme internationale fournit un cadre du SMSI pour la mise en œuvre de certains principes de l'OCDE, en utilisant le modèle PDCA et les processus décrits dans les Articles 4, 5, 6 et 8, tel qu'indiqué dans le Tableau B.1.

Tableau B.1 — Principes de l'OCDE et modèle PDCA

Principe de l'OCDE	Processus SMSI et phase PDCA correspondants
Sensibilisation Il convient que les parties prenantes soient sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.	Cette activité fait partie intégrante de la phase Déployer (voir 4.2.2 et 5.2.2).
Responsabilité Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.	Cette activité fait partie intégrante de la phase Déployer (voir 4.2.2 et 5.1).
Réaction Il convient que les parties prenantes agissent avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.	Il s'agit, pour partie, d'une activité de surveillance de la phase Contrôler (voir 4.2.3 et 6 à 7.3, ainsi que d'une activité de réaction de la phase Agir (voir 4.2.4 et 8.1 à 8.3). Ces activités peuvent également être couvertes par certains aspects des phases Planifier et Contrôler.
Évaluation des risques Il convient que les parties prenantes procèdent à des évaluations des risques.	Cette activité fait partie intégrante de la phase Planifier (voir 4.2.1) et la réévaluation du risque fait partie intégrante de la phase Contrôler (voir 4.2.3 et 6 à 7.3).
Conception et mise en œuvre de la sécurité Il convient que les parties prenantes intègrent la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.	Une fois effectuée l'appréciation du risque, des mesures sont sélectionnées pour le traitement des risques comme partie intégrante de la phase Planifier (voir 4.2.1). La phase Déployer (voir 4.2.2 et 5.2) couvre alors la mise en œuvre et l'application de ces mesures.
Gestion de la sécurité Il convient que les parties prenantes adoptent une approche globale de la gestion de la sécurité.	Le management du risque est un processus qui inclut la prévention, la détection et la réaction aux incidents, ainsi qu'une mise à jour, un réexamen et un audit permanents. Tous ces aspects sont contenus dans les phases Planifier, Déployer, Contrôler et Agir.
Réévaluation Il convient que les parties prenantes réexaminent et réévaluent la sécurité des systèmes et réseaux d'information, et introduisent les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.	La réévaluation de la sécurité de l'information fait partie intégrante de la phase Contrôler (voir 4.2.3 et 6 à 7.3) au cours de laquelle il convient de procéder à des réexamens réguliers pour contrôler l'efficacité du SMSI, et l'amélioration de la sécurité fait partie intégrante de la phase Agir (voir 4.2.4 et 8.1 à 8.3).

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**

Bibliographie

Publications de normes

[1] ISO 9001:2000, *Systèmes de management de la qualité — Exigences*.

[2] ISO/CEI 13335-1:2004, *Technologies de l'information — Techniques de sécurité — Gestion de la sécurité des technologies de l'information et des communications — Partie 1: Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications*

[3] ISO/CEI TR 13335-3:1998, *Technologies de l'information — Lignes directrices pour la gestion de sécurité IT — Partie 3: Techniques pour la gestion de sécurité IT*

[4] ISO/CEI TR 13335-4:2000, *Technologies de l'information — Lignes directrices pour la gestion de sécurité IT — Partie 4: Sélection de sauvegardes*

[5] ISO 14001:2004, *Systèmes de management environnemental — Exigences et lignes directrices pour son utilisation*

[6] ISO/CEI TR 18044:2004, *Technologies de l'information — Techniques de sécurité — Gestion d'incidents de sécurité de l'information*

[7] ISO 19011:2002, *Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*

[8] ISO/CEI Guide 62:1996, *Exigences générales relatives aux organismes gérant l'évaluation et la certification/enregistrement des systèmes qualité*

[9] ISO/CEI Guide 73:2002, *Management du risque — Vocabulaire — Principes directeurs pour l'utilisation dans les normes*

Normes publiées

[10] OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org*

[11] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

[12] Deming W.E., *Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986*