PROJET DE NORME INTERNATIONALE ISO/DIS 34001

ISO/TC **247** Secrétariat: **ANSI**

Début de vote **2013-03-25** Vote clos le **2013-06-25**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Système de management de la sécurité

Security Management System

ICS 03.100.01

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

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

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres 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 ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO 34001 a été élaborée par le comité technique ISO/TC 247, *Mesures de prévention et de contrôle de la fraude*, sous-comité SC , .

Introduction

Les organismes, de tous types et de toutes tailles, ont intérêt à réduire le plus possible les risques pour leurs actifs tangibles et intangibles en les protégeant des actes malveillants et frauduleux. Ces actes frauduleux incluent les actes délibérés d'individus et les actes involontaires facilitant un acte frauduleux par d'autres personnes. La protection des actifs tangibles et intangibles inclut d'éviter qu'ils ne tombent en des mains et des esprits non autorisés (dommages induits) car les organismes eux-mêmes et d'autres comptent dessus et dans certains cas en dépendent de façon critique. Les informations personnelles d'identification susceptibles d'être utilisées pour commettre un vol d'identité ainsi que les matériaux spéciaux qui sont critiques pour les caractéristiques de performances et d'exclusivité propres à un produit sont des exemples d'informations et d'actifs physiques sensibles qui doivent être protégés. Afin de protéger les actifs et les informations sensibles et d'éviter tout dommage induit, il convient que les organismes soient capables de résister, dans une plus ou moins grande mesure, à toutes les formes courantes d'actes de menace et de malveillance. Il convient que les organismes soient également capables de résister aux formes d'actes de menace et de malveillance qui sont spécifiques à l'organisme du fait de l'emplacement géographique, de la juridiction, du secteur, de l'industrie, de la nature du produit, du service ou de l'utilisation finale. La fraude peut également se produire hors du contrôle direct d'un organisme par le biais de la contrefaçon ou du détournement de ses produits. L'exposition totale aux menaces courantes et spécifiques représente le profil de risque d'un organisme en matière d'actifs et d'informations sensibles. Afin de résister efficacement à toutes les menaces contenues dans un profil, il est nécessaire de recourir à une expertise spécifique en management de la sûreté et à des activités, processus, politiques, procédures, infrastructures, systèmes et cultures de management particuliers. À cette fin, la présente Norme internationale spécifie des exigences normatives pour la mise en œuvre de fonctions et de processus de management général et de management de la sûreté qui, ensemble, permettent à un organisme de planifier, d'appliquer, de tenir à jour et d'améliorer un système complet de management de la sûreté.

Les organismes peuvent utiliser cette norme de système de management pour établir et mettre en œuvre une stratégie adaptée à leur profil de risque et à leurs exigences commerciales.

Les organismes ou les parties utilisatrices peuvent utiliser cette norme pour spécifier des exigences en matière de résistance aux menaces. Une partie prenante, un partenaire commercial, une partie utilisatrice ou un employé d'un organisme peuvent vérifier la résistance au niveau de menace en évaluant la conformité à la présente norme de management de la sûreté.

La présente Norme internationale est destinée à tous les organismes devant gérer un risque de sûreté. Elle n'inclut pas les normes sectorielles spécifiques ni les pratiques recommandées relatives par exemple à la fraude financière, la fraude liée à la gestion de projet et la fraude liée à l'information. Il existe des normes qui sont spécifiques à ces domaines.

La relation entre sûreté, sécurité et qualité dans cette norme est un concept important à assimiler.

Un système de management de la sûreté n'est pas un système de management de la qualité. Une norme de système de management de la qualité vise à définir et mettre en œuvre les processus nécessaires pour produire de façon constante un produit conforme à une spécification.

Une norme de système de management de la sûreté n'est pas une norme de sécurité car elle se rapporte aux attributs d'un produit sûr à consommer ou à utiliser. Il convient qu'une norme de sécurité définisse les pratiques et processus qui rendront un produit sûr à consommer ou à utiliser.

La présente norme de système de management de la sûreté a pour objectif de fournir un cadre permettant aux organismes de gérer les risques d'actes frauduleux, favorisant ainsi la livraison de produits et services sûrs et de qualité. Cette différence d'objectif est significative entre une norme de système de management de la sûreté et une norme de système de management de la qualité ou de la sécurité.

La présente Norme internationale a été conçue pour pouvoir être intégrée aux systèmes de management de la qualité, de la sécurité, de l'environnement, de la sécurité de l'information, de la sûreté de la chaîne d'approvisionnement et autres systèmes de management au sein d'un organisme. Un système de management conçu de manière adéquate peut donc satisfaire aux exigences de toutes ces normes. Les organismes ayant adopté une approche ISO des systèmes de management (par exemple, conformément à l'ISO 9001:2008, l'ISO 14001:2004, l'ISO/CEI 27001:2005 ou l'ISO 28000:2007) peuvent être à même d'utiliser leur système de management existant comme base pour le système de management de la sûreté prescrit dans la présente Norme internationale.

La présente Norme internationale traite des risques liés aux individus et organismes cherchant à perturber le cours normal des opérations ou à tirer un bénéfice non autorisé de la commission d'actes frauduleux.

La gestion des risques d'actes frauduleux est essentielle pour assurer la qualité et la sécurité des produits et services d'un organisme. La présente Norme internationale permet aux organismes d'établir les mesures de prévention et de contrôle de la fraude nécessaires pour se protéger des actes frauduleux internes et externes. Elle vient en complément des autres normes ISO de management du risque de sûreté relatives à la sécurité de l'information et à la sûreté de la chaîne d'approvisionnement. Afin d'établir une solide stratégie, l'organisme doit définir, mettre en œuvre et tenir à jour un système de management prenant en compte les enjeux liés à la gestion des risques identifiés lors de son appréciation du risque, de manière à réduire le plus possible la vraisemblance et les conséquences d'actes frauduleux susceptibles d'être préjudiciables à l'organisme et à ses actifs, aussi bien tangibles qu'intangibles.

La présente Norme internationale fournit une approche holistique des questions de sûreté en rapport avec la fraude en partant du principe que la fraude est tout acte commis par des individus ou des organismes visant à causer un préjudice financier, social ou physique. Cette Norme internationale fournit un cadre permettant à l'organisme de se protéger des actes frauduleux pour préserver le cours normal des opérations. Elle est applicable à la fois au secteur public et privé. Elle est destinée à être compatible avec les normes ISO existantes relatives à la sûreté (ces normes sont indiquées dans le présent document). La présente Norme internationale est également destinée à venir à l'appui des futures normes relatives à la sûreté.

La présente Norme internationale est applicable à toutes les tailles et tous les types d'organismes dans le secteur privé, à but non lucratif et public. Il est souhaitable que l'adoption d'un système de management de la sûreté relève d'une décision stratégique de l'organisme. La conception et la mise en œuvre du système de management de la sûreté d'un organisme tiennent compte :

a) du contexte interne et externe dans lequel il opère,

b) de ses besoins propres et de ceux de ses parties prenantes,

c) de ses objectifs,

d) des produits et services fournis,

e) du caractère sensible de ses actifs et informations,

f) de ses processus et de son secteur industriel, et

g) de sa taille et de sa structure organisationnelle,

h) des exigences légales nationales applicables.

La démarche qui s'appuie sur un système de management incite les organismes à analyser les exigences organisationnelles et les exigences des parties prenantes et à définir les processus qui contribuent à l'établissement d'une solide stratégie en matière de sûreté. Un système de management peut fournir le cadre d'amélioration continue permettant d'accroître la probabilité de préserver la sûreté et l'intégrité des actifs. Il apporte, à l'organisme et à ses parties prenantes, la confiance en l'aptitude de l'organisme à fournir un environnement sûr et sécurisé qui satisfait aux exigences organisationnelles et aux exigences des parties prenantes.

La présente norme adopte une approche processus pour l'établissement, la mise en œuvre, l'application, la surveillance, la revue, la tenue à jour et l'amélioration du système de management de la sûreté d'un organisme. Un organisme a besoin d'identifier et de gérer un grand nombre d'activités afin de fonctionner efficacement. 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.

Une « 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 relative au management de la sûreté présentée dans la présente norme incite ses utilisateurs à insister sur l'importance de :

a) comprendre les exigences d'un organisme en matière de risque, de sûreté et de protection des actifs ;

b) établir une politique et des objectifs pour gérer les risques ;

c) mettre en œuvre et appliquer des moyens de maîtrise pour gérer les risques d'un organisme dans le contexte de la mission de l'organisme ;

d) surveiller et passer en revue les performances et l'efficacité du système de management de la sûreté ; et

e) e) l'amélioration continue sur la base de mesures objectives.

La présente norme adopte le concept de la « roue de Deming », désigné en anglais par « Plan-Do-Check-Act (PDCA) », qui est appliqué pour structurer les processus des systèmes de management de la sûreté. La Figure 1 (à ajouter ultérieurement) illustre la manière dont un système de management de la sûreté prend en entrée les exigences et les attentes des parties intéressées en matière de management de la sûreté et, au moyen des actions et processus nécessaires, donne des résultats en termes de management du risque qui satisfont aux exigences et aux attentes. La Figure 1 illustre également les liens dans les processus présentés dans le corps de la norme.

Tableau 1 — Roue de Deming

Planifier (établir le système de management)	Établir la politique, les objectifs, les processus et les procédures du système de management relatifs à la gestion du risque et à l'amélioration du système de management de la sûreté, et permettant de fournir des résultats conformes aux politiques et objectifs généraux d'un organisme.
Développer (mettre en œuvre et appliquer le système de management)	Mettre en œuvre et appliquer la politique, les moyens de maîtrise, les processus et les procédures du système de management.
Contrôler (surveiller et passer en revue le système de management)	Évaluer et mesurer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique du système de management, et rapporter les résultats à la direction pour revue.
Agir (tenir à jour et améliorer le système de management)	Entreprendre des actions correctives et préventives en fonction des résultats de l'audit interne et de la revue de direction du système de management, afin d'assurer l'amélioration continue du système de management.

La conformité à la présente norme peut être vérifiée par un processus d'audit compatible et cohérent avec la méthodologie de l'ISO 9001:2000, l'ISO 14001:2004, l'ISO/CEI 27001:2005 et/ou avec la roue de Deming.

Système de management de la sécurité

1 Domaine d'application

La présente Norme internationale traite de la gestion des risques d'actes frauduleux auxquels sont exposés les actifs tangibles et intangibles d'un organisme. Cela comprend les actes de :

a) tromperie délibérée,

b) malveillance,

c) négligence volontaire, et

d) facilitation involontaire d'activités frauduleuses.

Les exigences spécifiées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à tout organisme (ou partie d'un organisme), quels que soient le type, la taille et la nature de l'organisme. L'étendue de l'application de ces exigences dépend de l'environnement opérationnel, du portefeuille de produits et services, du profil de risque et de la complexité de l'organisme.

La présente Norme internationale spécifie les exigences relatives à un système de management de la sûreté pour la prévention et le contrôle de la fraude, permettant à un organisme d'établir et de mettre en œuvre des politiques, des objectifs et des programmes. Elle s'applique aux risques et aux impacts d'actes frauduleux identifiés par l'organisme comme devant être contrôlés, influencés ou réduits. Elle ne définit pas elle-même de critères de performances spécifiques.

La présente Norme internationale est destinée à aider les organismes à :

a) développer une politique de sûreté ;

b) établir des objectifs, des procédures et des processus permettant de tenir les engagements pris dans la politique ;

c) démontrer la conformité aux exigences légales et autres exigences ;

d) assurer la compétence, la sensibilisation et la formation ;

e) évaluer les performances et entreprendre des actions en conséquence pour les améliorer ;

f) démontrer la conformité du système de management aux exigences de la présente Norme internationale ; et

g) établir et appliquer un processus d'amélioration continue.

La présente Norme internationale est applicable à tout organisme souhaitant :

a) développer, mettre en œuvre, tenir à jour et améliorer un système de management de la sûreté pour la prévention et le contrôle de la fraude ;

b) s'assurer lui-même de sa conformité à sa politique de sûreté déclarée ;

c) démontrer la conformité à la présente Norme internationale par :

i) la réalisation d'une autodétermination et d'une autodéclaration ; ou

ii) la recherche d'une confirmation de sa conformité par des parties ayant un intérêt dans l'organisme (telles que les clients) ; ou

iii) la recherche d'une confirmation de son autodéclaration par une partie externe à l'organisme ; ou

iv) la recherche de la certification/enregistrement de son système de management de la sûreté pour la prévention et le contrôle de la fraude par un organisme externe.

2 Références normatives

Aucune référence normative n'est citée pour le moment. Cet article a été inclus afin que la numérotation des articles soit identique à celle des autres normes ISO de systèmes de management.

3 Termes et définitions

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

3.01
organisme
personne ou groupe de personnes disposant de fonctions qui lui sont propres en termes de responsabilité, autorité et relations en vue d'atteindre ses objectifs (3.08)

Note 1 à l'article Le concept d'organisme comprend (mais n'est pas limité à) : travailleur indépendant, compagnie, société, firme, entreprise, autorité, partenariat, organisation caritative ou institution, ou une combinaison des entités précédentes, qu'elle soit constituée/immatriculée ou non, publique ou privée.

3.02
partie intéressée (terme préféré)
partie prenante (terme admis)
personne ou organisme (3.01) susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

3.03
exigence
besoin ou attente formulés, habituellement implicites, ou imposés

Note 1 à l'article Habituellement implicite » signifie qu'il est d'usage ou de pratique courante pour l'organisme et les parties intéressées de considérer le besoin ou l'attente en question comme implicite.

Note 2 à l'article Une exigence spécifiée est une exigence qui est formulée, par exemple dans une information documentée.

3.04
système de management
ensemble d'éléments corrélés ou interactifs d'un organisme (3.01) permettant d'établir des politiques (3.07) et des objectifs (3.08), ainsi que des processus (3.12) pour atteindre ces objectifs

Note 1 à l'article Un système de management peut aborder une seule ou plusieurs disciplines.

Note 2 à l'article Les éléments du système comprennent la structure organisationnelle, les rôles et responsabilités, la planification, le fonctionnement, etc.

Note 3 à l'article Le domaine d'application d'un système de management peut comprendre l'ensemble de l'organisme, des fonctions spécifiques et identifiées de l'organisme, des sections spécifiques et identifiées de l'organisme, ou une ou plusieurs fonctions dans un groupe d'organismes.

3.05
direction générale
personne ou groupe de personnes qui oriente et contrôle un organisme (3.01) au plus haut niveau

Note 1 à l'article La direction générale a le pouvoir de déléguer son autorité et de fournir des ressources au sein de l'organisme.

Note 2 à l'article Si le domaine d'application du système de management (3.04) ne couvre qu'une partie d'un organisme, alors la direction générale fait référence aux personnes qui orientent et contrôlent cette partie de l'organisme.

3.06
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

3.07
politique
intentions et orientations données à l'organisme (3.01) et formalisées par sa direction générale (3.05)

3.08
objectif
résultat à atteindre

Note 1 à l'article Un objectif peut être stratégique, tactique ou opérationnel.

Note 2 à l'article Les objectifs peuvent concerner différents domaines (financier, environnemental, santé et sécurité, etc.) et peuvent s'appliquer à différents niveaux (stratégique, organisme dans son ensemble, projet, produit, processus (3.12), etc.).

Note 3 à l'article Un objectif peut être exprimé autrement, par exemple comme un résultat escompté, un but, un critère opérationnel, comme un objectif de sûreté, ou en recourant à d'autres termes ayant la même signification (par exemple finalité, but ou cible).

Note 4 à l'article Dans le contexte d'un système de management de la sûreté, les objectifs de sûreté sont établis par l'organisme, en cohérence avec sa politique de sûreté, afin d'atteindre des résultats spécifiques.

3.09
risque
effet de l'incertitude

Note 1 à l'article Un effet est un écart, positif et/ou négatif, par rapport à une attente.

Note 2 à l'article L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Note 3 à l'article Un risque est souvent caractérisé en référence à des événements (ISO Guide 73, 3.5.1.3) et des conséquences (ISO Guide 73, 3.6.1.3) potentiels ou à une combinaison des deux.

Note 4 à l'article Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance (ISO Guide 73, 3.6.1.1).

3.10
compétence
aptitude à mettre en pratique des connaissances et un savoir-faire pour obtenir les résultats escomptés