PROJET
FINAL

NORME INTERNATIONALE

ISO/FDIS 22342

ISO/TC **292**

Secrétariat: **SIS**

Début de vote:
2023-01-31

Vote clos le:
2023-03-28

Sécurité et résilience — Sûreté préventive — Lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme

Security and resilience — Protective security — Guidelines for the development of a security plan for an organization

Numéro de référence
ISO/FDIS 22342:2023(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

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 (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée 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. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 292, *Sécurité et résilience*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Tous les organismes cherchent à gérer les risques de sûreté dans leur environnement afin d'assurer des niveaux de protection appropriés de leurs actifs, de préserver les intérêts des parties intéressées et d'atteindre leurs objectifs.

Les organismes ont parfois besoin d'établir et de tenir à jour une approche structurée de la sûreté.

L'objectif d'un plan de sûreté est d'assurer que toutes les actions et tous les contrôles appropriés sont en place pour protéger l'organisme contre les menaces à sa sécurité.

Le présent document donne des lignes directrices pour l'implémentation d'un plan de sûreté dont la structure inclut les recommandations pour une architecture de sûreté préventive. Ainsi, le plan de sûreté peut être intégré efficacement dans un système de management existant.

L'intégration des processus de management du risque de l'organisme au modèle de plan de sûreté, contribue à une gestion appropriée de la sûreté. Ce plan de sûreté est conçu pour attribuer l'imputabilité et la responsabilité de même pour guider la mise en œuvre des contrôles afin de protéger l'organisme contre les risques de sûreté.

Une approche planifiée, adaptative et agile permet d'apporter des solutions à des situations non anticipées. Les menaces pour la sûreté sont dynamiques et souvent inattendues; par conséquent, le présent document introduit des éléments à la fois techniques et humains pour une approche planifiée adaptative et agile.

L'objet de ce document est de fournir les éléments fondamentaux nécessaires pour améliorer et soutenir la protection d'un organisme.

Sécurité et résilience — Sûreté préventive — Lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme

1 Domaine d'application

Le présent document fournit des recommandations pour l'élaboration et la tenue à jour des plans de sûreté.

Le plan de sûreté décrit comment un organisme établit une planification de la sûreté efficace et comment il peut intégrer la sûreté dans les pratiques organisationnelles de management du risque.

Le présent document s'applique à tous les organismes, quels que soient leur type, leur taille et leur nature, qu'ils appartiennent au secteur privé, au secteur public ou au secteur non lucratif, qui souhaitent élaborer des plans de sûreté efficaces de manière cohérente.

Le présent document s'applique à tout organisme qui souhaite implémenter des mesures destinées à protéger ses actifs contre les actes de malveillance et à atténuer les risques associés.

Le présent document ne fournit pas de critères spécifiques permettant d'identifier la nécessité d'implémenter ou d'améliorer les mesures de prévention et de protection contre les actes de malveillance. Il ne s'applique ni aux services ni aux opérations fournis par les sociétés de sécurité privées.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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 22300, *Sécurité et résilience — Vocabulaire*

ISO 31000, *Management du risque — Lignes directrices*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 22300 et l'ISO 31000 ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
besoin d'en connaître
besoin d'avoir accès à des informations spécifiques sur la base d’une exigence fonctionnelle ou opérationnelle, impliquant un processus actif de détermination du niveau de sûreté des informations, et des droits d'accès à ces informations

4 Planification de la sûreté

Il convient que l'organisme crée, implémente et tienne à jour un plan de sûreté pour gérer les activités sur la base d'une analyse du risque de sûreté en phase avec sa mission.

Il convient que le plan de sûreté:

— soit propre à chaque organisme;

— soit basé sur des stratégies et des objectifs de sûreté concernant les menaces et les vulnérabilités;

— soit passé en revue et approuvé officiellement par la direction avant son implémentation;

— anticipe la nécessité de faire face à long terme à des incidents relatifs à la sûreté, en intégrant des procédures spéciales et des structures adaptatives afin d'être en mesure de faire face de façon adéquate à pareils événements perturbateurs.

L'organisme peut utiliser un unique plan de sûreté ou un plan de sûreté global comportant des plans plus détaillés.

NOTE Un plan de sûreté unique n'est pas toujours réalisable en raison de la taille de l'organisme ou de la complexité de son activité.

5 Composants du plan de sûreté

5.1 Généralités

Le présent article fournit des recommandations sur la façon d'élaborer les différents composants d'un plan de sûreté. Il se compose des paragraphes suivants, qui fournissent des recommandations détaillées relatives:

— à la gouvernance (voir 5.2);

— au management du risque (voir 5.3);

— aux contrôles de sûreté (voir 5.4);

— au processus relatif aux contrôles de sûreté (voir 5.5);

NOTE L'ISO 28000:2022, 8.6 contient également des informations concernant le contenu d'un plan de sûreté.

5.2 Gouvernance

5.2.1 Généralités

Il convient que l'organisme détermine comment administrer le plan de sûreté. Cela inclut la prise en compte des aspects suivants:

— objectifs de sûreté (voir 5.2.2);

— domaine d'application du plan de sûreté (voir 5.2.3);

— direction (voir 5.2.4);

— impact réglementaire et juridique (voir 5.2.5);

— rôles, imputabilités et responsabilités (voir 5.2.6);

— communication (voir 5.2.7);

— information documentée (voir 5.2.8);

— établissement des rapports (voir 5.2.9);

— évaluation (voir 5.2.10);

— amélioration continue (voir 5.2.11).

5.2.2 Objectifs de sûreté

Il convient que l'organisme définisse les objectifs sûreté du plan, prenant en compte:

— les objectifs et priorités pour une activité étendue;

— le cadre de la sûreté préventive;

— les politiques de sûreté associées;

— le risque de sûreté.

5.2.3 Domaine d'application du plan de sûreté

Il convient que l'organisme détermine les limites et l'applicabilité du plan de sûreté afin d'établir son domaine d'application.

Cela inclut le fait de décider si le plan de sûreté s'applique à tout ou partie de l'organisme ou s'il ne s'applique qu'à une durée spécifique d'un projet.

Il convient que le domaine d'application du plan de sûreté tienne compte de tout autre processus de management du risque organisationnel concernant les violations ou les menaces pour la sécurité.

Il convient que le domaine d'application du plan de sûreté tienne compte de plusieurs critères incluant:

— les missions et spécificités des opérations de l'organisme;

— les problèmes externes et internes;

— le personnel concerné (y compris le personnel externe);

— les actifs matériels et immatériels à protéger;

— les lieux et espaces de l'organisme;

— les lieux de déplacement ou activités en dehors des installations de l'organisme (si nécessaire);

— les activités en fonction de leur nature et de leur relation avec les aspects sûreté;

— et tout autre critère pertinent.

Il convient en outre que le plan de sûreté indique toutes les exclusions applicables. Il convient que le domaine d'application du plan de sûreté soit disponible sur la base d'un besoin d'en connaître.

5.2.4 Direction

Il convient que la direction générale:

— spécifie la direction responsable du plan de sûreté et de sa gestion, cela comprend l'attribution de la responsabilité pour la création, la tenue à jour et l'exécution du plan de sûreté à la fonction sûreté de l'organisme, et cela tient les personnes désignées comme responsables de leur performance;

— s'assure que le plan de sûreté contienne des recommandations pour que la direction générale reçoive des rapports et revues appropriés sur l'état de la sûreté de l'organisme et que des actions d'amélioration soient entreprises en réponse à ces revues;

— se coordonne avec les gestionnaires d'actifs et le personnel chargé du management de la sûreté lors de l'élaboration du plan de sûreté afin de s'assurer que celui-ci soutienne les objectifs généraux de l'organisme.

— communique également son engagement à la sûreté au reste de l'organisme afin de promouvoir un sentiment partagé d'unité sur l'importance de la sûreté;

— fournisse les ressources nécessaires à la mise en œuvre d'un plan de sûreté.

5.2.5 Aspect réglementaire et juridique

Il convient que l'organisme identifie toute obligation légale, réglementaire et contractuelle applicable. Il convient également d'en tenir compte lors de la mise en œuvre d'un plan de sûreté. Il convient que l'organisme soit en contact étroit avec les autorités et leur communique les responsabilités, les dispositions et autres éléments clés.

5.2.6 Rôles, imputabilités et responsabilités

Il convient que l'organisme définisse et documente les rôles, responsabilités et autorités en matière de sûreté pour l'exécution du plan de sûreté. Cela inclut de spécifier:

— les compétences requises pour l'exécution du plan;

— un niveau de compétence attribué et défini pour chaque rôle;

— la relation entre l'équipe sûreté interne et les parties intéressées externes.

Il convient que le plan de sûreté aligne les dispositions de gouvernance de la sûreté sur la gouvernance générale de l'organisme. Le cas échéant, il convient de définir les relations avec les autorités de sûreté externes ayant un rôle de gouvernance. Il convient que les exemptions aux dispositions sûreté prédéfinies soient énumérées, documentées et passées en revue.

5.2.7 Communication

Il convient que l'organisme communique les contenus et obligations du plan de sûreté aux parties intéressées pertinentes, y compris:

— les relations de confiance internes et externes de la direction pour partager les informations stratégiques, les bonnes pratiques et les enseignements tirés;

— les réponses aux urgences et aux crises en matière de sûreté;

— les rôles et les responsabilités.

Il convient que l'organisme élabore également une politique de partage des informations relatives à sa sécurité et l'application du principe de «besoin d'en connaître».

5.2.8 Informations documentées

Il convient que l'organisme documente les informations nécessaires à l'efficacité du plan, y compris:

— le domaine d'application du plan de sûreté;

— les décisions passées relatives aux risques de sûreté (y compris les risques partagés et résiduels), les traitements appliqués et leur efficacité;

— les enseignements tirés des décisions passées afin de permettre à l'organisme de prendre les mesures pertinentes pour une amélioration continue;

— les politiques et procédures pertinentes pour le plan de sûreté.

5.2.9 Établissement des rapports

Il convient d'inclure dans le plan de sûreté des recommandations visant à garantir que la direction reçoive des rapports appropriés concernant l'exécution du plan.

5.2.10 Évaluation

Il convient que l'évaluation du plan de sûreté prenne en compte:

— l'approche de l'organisme en matière de management du risque;

— les objectifs stratégiques et de sûreté;

— les ressources nécessaires, y compris le personnel, les besoins en formation et le niveau de compétence requis;

— les résultats de l'évaluation.

Il convient que l'organisme évalue l'efficacité du plan de sûreté sur la base:

— de ce qu'il est nécessaire d'évaluer;

— des méthodes à utiliser pour l'évaluation;

— de la manière dont il convient d'effectuer, d'analyser et de rapporter l'évaluation;

— de la fréquence définie des évaluations (par exemple: situations normales et situations d'urgence);

— de qui est autorisé à évaluer le plan de sûreté.

5.2.11 Amélioration continue

Il convient que l'organisme améliore de façon continue le plan de sûreté:

— en recherchant activement des opportunités d'amélioration, même si elles ne sont pas provoquées par des vulnérabilités liées à la sûreté et des menaces de sûreté imminentes ou des violations de sûreté en cours;

— en prenant en compte:

  — des ajustements apportés au plan, y compris en matière de risques et de contrôles;

  — des ressources disponibles pour le plan, y compris en matière de personnel, de matériels et d'installations.

5.3 Management du risque

5.3.1 Généralités

Traiter les risques pour permettre au plan de sûreté d'atteindre ses résultats escomptés nécessite une approche fondée sur le management du risque adaptée à l'organisme. Il convient que l'interaction avec la planification globale de l'organisme soit reconnue et cohérente.

En fonction du niveau de risque pour les actifs à protéger, il convient que les niveaux de protection requis soient définis pour les actifs et des contrôles implémentés et déterminés pour atteindre le niveau de risque acceptable convenu.

Il est recommandé à l'organisme de gérer son risque de sûreté en suivant le processus de gestion du risque décrit dans l'Article 6 de l'ISO 31000:2018, notamment:

— le domaine d'application, le contexte et les critères du risque de sûreté (voir 5.3.2);