PROJET FINAL
Norme internationale

ISO/FDIS 22340

Sécurité et résilience — Sûreté préventive — Lignes directrices pour une architecture et un cadre de sûreté préventive de l'entreprise

Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework

ISO/TC **292**

Secrétariat: **SIS**

Début de vote:
2024-07-15

Vote clos le:
2024-09-09

Numéro de référence
ISO/FDIS 22340:2024(fr)

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'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevet.

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 www.iso.org/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

Le présent document vise à répondre à un besoin global des organismes de formuler et d'intégrer leurs contrôles de sûreté préventive d'une manière qui soit fondée sur les principes de management du risque et stratégiquement alignée sur les intérêts de l'organisme. Il décrit en détail une architecture d'entreprise et un cadre intégré au sein desquels un ensemble divers de politiques, de processus et de pratiques liés à la sûreté peuvent être coordonnés.

La clarification de ce qu'est la sûreté préventive, de ce qu'elle signifie, de la manière dont elle peut être mise en œuvre et de la manière dont ses avantages peuvent être mesurés, sera utile aux membres du management, quel que soit leur secteur d'activité. Cela est particulièrement important pour les nombreux organismes qui ont consacré des ressources importantes à diverses mesures de sûreté qui n'ont pas nécessairement été coordonnées ou sous-tendues par l'ensemble des risques liés à la sûreté. Dans un environnement de sûreté de plus en plus complexe, le présent document vise à apporter des éclaircissements à cet égard et à fournir une base permettant d'obtenir de meilleurs résultats en matière de sûreté de l'entreprise.

Le présent document:

a) fournit des recommandations sur la manière dont les organismes et leurs membres du management peuvent mettre en œuvre et gérer des dispositifs de sûreté préventive cohérents;

b) démontre l'idée essentielle qu'un management efficace de la sûreté repose sur une compréhension du risque et l'application des principes de management du risque, et que la forme et la mise en œuvre des contrôles de sûreté (qui protègent les actifs d'un organisme) font partie intégrante du succès à long terme de l'organisme. La sûreté est un moteur de l'activité, et non un coût indirect pour l'organisme;

c) définit et détaille les éléments de la sûreté préventive, décrit un modèle de gouvernance de la sûreté préventive de l'entreprise et définit les rôles et responsabilités nécessaires pour obtenir des résultats en matière de sûreté préventive;

d) démontre l'importance cruciale de l'établissement et du maintien d'une culture organisationnelle soutenant des comportements positifs en matière de sûreté: où l'ensemble du personnel et des parties intéressées ont un sentiment d'appropriation partagée des résultats en matière de sûreté; et où tous sont autorisés et compétents pour agir dans l'intérêt de la sûreté de l'organisme et s'investissent dans la sûreté de l'organisme;

e) souligne l'importance de l'amélioration continue en ce qui concerne la sûreté préventive d'un organisme.

Le présent document s'applique à tout organisme et sera particulièrement utile à ceux qui ont éprouvé des difficultés à mettre en œuvre des cadres fondés sur le risque et adaptés à leur contexte de sûreté. Les organismes confrontés à de telles difficultés peuvent s'inspirer du présent document pour identifier et obtenir l'aide de services dûment compétents.

Les lignes directrices contenues dans le présent document ne fournissent pas de procédures détaillées au niveau technique ou opérationnel. En l'absence de normes à ce niveau, il convient que les organismes élaborent et mettent en œuvre des procédures sur la base des recommandations générales contenues dans le présent document et conformément aux meilleures pratiques aux niveaux national et international.

Sécurité et résilience — Sûreté préventive — Lignes directrices pour une architecture et un cadre de sûreté préventive de l'entreprise

1 Domaine d'application

Le présent document fournit des recommandations relatives à l'architecture de sûreté préventive de l'entreprise et au cadre des politiques, processus et types de contrôles en matière de sûreté préventive, nécessaires pour atténuer et gérer les risques liés à la sûreté dans l'ensemble des domaines de la sûreté préventive, y compris:

a) la gouvernance de la sûreté;

b) la sûreté du personnel;

c) la sécurité de l'information;

d) la cybersécurité;

e) la sûreté physique.

Le présent document est applicable à tout organisme.

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*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 22300 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
propriétaire d'un actif
personne qui, au sein de l'organisme, est responsable d'un actif donné

3.2
impact sur l'activité
impact sur la capacité d'un organisme ou d'un secteur à fonctionner résultant du fait que la confidentialité, l'intégrité ou la disponibilité des actifs ont été compromises

3.3
culture
valeurs et attitudes communes appliquées au sein d'un organisme par son personnel et les parties intéressées

Note 1 à l'article: Il est reconnu qu'un organisme a une culture qui, à des degrés divers, soutient et accepte la sûreté comme faisant partie des activités habituelles; et il convient que la promotion de cet élément de la culture de l'organisme soit l'objectif de la direction pour obtenir des résultats en matière de sûreté préventive.

3.4
cybersécurité
protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes numériques (matériels, logiciels et infrastructures associées) contre les accès numériques non autorisés, les dommages ou les utilisations abusives, ou les scénarios d'attaque qui impliquent l'exploitation délibérée des systèmes informatiques, des réseaux d'entreprise dépendant du numérique et des systèmes de contrôle

Note 1 à l'article: Ceci concerne une série de *domaines* (3.5) techniques, y compris, mais sans s'y limiter nécessairement, les *technologies de l'information et de la communication (TIC)* (3.9) et les technologies opérationnelles (TO).

3.5
domaine
sphère définie d'activité ou de connaissance en matière de *sûreté préventive* (3.17)

3.6
architecture de sûreté préventive de l'entreprise
structure documentée comprenant les modalités de gouvernance et les éléments du cadre de sûreté par lesquels les fonctions de sûreté préventive sont assurées et alignées stratégiquement sur les objectifs de l'organisme

3.7
cadre
structure de politiques, de processus et de spécifications conçue pour soutenir la réalisation d'un objectif

Note 1 à l'article: Dans cette optique, un cadre de sûreté préventive comprend et aligne tous les éléments de la politique et des processus de sûreté préventive, y compris la *gouvernance* (3.8) de la sûreté, la *sûreté du personnel* (3.15), la *sécurité de l'information* (3.12), la *cybersécurité* (3.4) et la *sûreté physique* (3.16).

3.8
gouvernance
système permettant de diriger et de contrôler

Note 1 à l'article: Il s'agit des processus par lesquels les organismes sont dirigés, contrôlés et tenus de rendre des comptes, englobant l'autorité, l'imputabilité, la gérance, le leadership, l'orientation et le contrôle exercés au sein de l'organisme.

3.9
technologies de l'information et de la communication
TIC
technologie d'extraction, de stockage, d'accès, d'analyse et de transmission des informations

[SOURCE: ISO/IEC 30071-1:2019, 3.2.5]

3.10
actif informationnel
connaissances ou données ayant de la valeur pour l'individu ou l'organisme (y compris la propriété intellectuelle), et qui sont définies et gérées de manière à pouvoir être comprises, partagées, protégées et utilisées

3.11
cycle de vie de l'information
processus par lequel l'information est gérée dans le temps, depuis sa création jusqu'à son élimination finale (élimination, destruction ou archivage), en passant par sa réception, sa distribution, son utilisation et sa tenue à jour, en fonction de l'impact sur l'activité de la réduction ou de la perte de la confidentialité, de l'intégrité ou de la disponibilité de l'information

3.12
sécurité de l'information
protection et préservation de la confidentialité, de l'intégrité et de la disponibilité de tous les *actifs informationnels* (3.10), y compris les informations en transit (par exemple, la sécurité transactionnelle), la sécurité numérique et la *cybersécurité* (3.4)

Note 1 à l'article: La sécurité de l'information concerne la sécurité des informations sous toutes leurs formes (y compris les communications écrites et orales), les systèmes numériques, les *technologies de l'information et de la communication (TIC)* (3.10) et les *technologies opérationnelles (TO)*.

Note 2 à l'article: D'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent être incluses.

[SOURCE: ISO/IEC 27000:2018, 3.28, modifié — La définition a été élargie et la Note 1 à l'article a été ajoutée.]

3.13
mesure
action ou moyens permettant d'éliminer les dangers ou de réduire les risques

[SOURCE: Guide ISO/IEC 51:2014, 3.13, modifié — L'exemple a été supprimé.]

3.14
besoin de savoir
nécessité d'accéder à des informations spécifiques pour répondre à une exigence commerciale ou opérationnelle, conformément à un processus actif de détermination du niveau de sûreté des informations et des personnes ayant le droit d'accéder à ces informations

3.15
sûreté du personnel
processus permettant d'obtenir et de conserver l'assurance qu'une personne est éligible et apte (honnêteté, fiabilité, maturité, résilience, loyauté et compétence en matière de sûreté) à accéder aux actifs de l'organisme

3.16
sûreté physique
combinaison de *contrôles de sûreté* (3.19) physiques visant à réduire le risque d'accès non autorisé, à protéger les actifs et à se prémunir contre un éventuel incident de sûreté

3.17
sûreté préventive
processus et activités qui protègent les actifs contre les actes de malveillance, l'impact des incidents non intentionnels et d'autres événements susceptibles de causer des dommages

Note 1 à l'article: La sûreté préventive comprend les domaines suivants: la *gouvernance* (3.8) de la sûreté, la *sûreté du personnel* (3.15), la *sécurité de l'information* (3.12), la *cybersécurité* (3.4) et la *sûreté physique* (3.16).

3.18
responsable de la sûreté
RS
personne désignée au sein de la direction de l'organisme comme unique responsable de la gestion du *risque lié à la sûreté* (3.21) de l'organisme

Note 1 à l'article: Ayant la responsabilité de la gestion du risque lié à la sûreté de l'organisme, le RS rend compte à la direction de l'exécution de cette tâche. La direction rend compte à son tour des performances globales de l'organisme en général.

Note 2 à l'article: Le RS est chargé de veiller à ce que la fonction de sûreté de l'organisme soit gérée efficacement et donne à la direction l'assurance que les risques liés à la sûreté sont gérés de manière active.

Note 3 à l'article: Une *gouvernance* (3.8) appropriée exige que le RS dispose de l'autorité, des ressources et des compétences nécessaires pour exercer cette responsabilité; et qu'il soit membre de la direction ou qu'il ait un accès effectif à celle-ci.

3.19
contrôle de sûreté
politique, processus, ou application tangible ou intangible d'une réduction du risque qui, sur la base d'une évaluation, est mis en œuvre pour traiter le risque en réduisant ou en maintenant la probabilité qu'un risque lié à la sûreté se réalise, à des niveaux ou dans des fourchettes spécifiques

Note 1 à l'article: Cela comprend, sans s'y limiter, les contrôles d'accès numérique et physique, les alarmes, la surveillance active et passive, la vérification et autres outils d'évaluation du personnel.

Note 2 à l'article: Un traitement en matière de sûreté est l'application ou la mise en œuvre effective d'un ou plusieurs contrôles de sûreté dans le but d'atteindre un niveau de risque acceptable.

3.20
sûreté en profondeur
défense en profondeur
protection en profondeur
utilisation de multiples *contrôles de sûreté* (3.19) préventive par couches dans l'ensemble de l'entreprise afin de protéger les actifs

Note 1 à l'article: Cette approche reconnaît que la force d'un système n'est pas plus grande que son point le plus faible et garantit qu'en cas de défaillance d'un élément de contrôle, d'autres *mesures* (3.13) de défense sont en place pour continuer à assurer la protection.

3.21
risque lié à la sûreté
possibilité que des acteurs malveillants (ou toute action ou tout événement non intentionnel) portent atteinte aux actifs d'un organisme ou aboutissent à les compromettre, à les perdre ou à les rendre indisponibles, ou réduisent l'efficacité des *contrôles de sûreté* (3.19)

Note 1 à l'article: Voir *menace pour la sûreté* (3.22).

Note 2 à l'article: Cette définition est inspirée de la définition du risque selon l'ISO 31000:2018, 3.1, dans le contexte du risque lié à la sûreté, en ce que l'incertitude relative à l'intention et à la capacité des acteurs malveillants et la vulnérabilité à leurs actions peuvent avoir une incidence sur les objectifs.

3.22
menace pour la sûreté
menace qui survient lorsque les intentions et les capacités d'acteurs malveillants sont mises en œuvre et se heurtent aux vulnérabilités des *contrôles de sûreté* (3.19) préventive ou des systèmes intrinsèques d'un organisme

Note 1 à l'article: Une vulnérabilité peut être inhérente à un actif ou à un processus ou être causée par un événement ou une circonstance quelconque, y compris un événement naturel ou un accident.

Note 2 à l'article: La menace est parfois considérée comme analogue au danger (source potentielle de dommage), bien que dans le contexte de la sûreté, le danger se réfère généralement à des matériaux ou des outils préexistants dans l'environnement d'exploitation qui peuvent être utilisés par un acteur malveillant, tels que des explosifs, des logiciels malveillants, etc.

3.23
vérification de sûreté
processus visant à vérifier l'identité du personnel et à fournir l'assurance qu'il est éligible et apte à accéder aux actifs de l'organisme

4 Architecture de sûreté préventive de l'entreprise

4.1 Généralités

La sûreté préventive est optimisée lorsqu'elle est alignée sur les principes de sûreté préventive et pilotée par la direction de l'organisme. Dans cette optique, il convient que l'organisme mette en œuvre des modalités de gouvernance qui permettent d'apprécier la sûreté au niveau de l'entreprise et fournissent un cadre de politiques, de processus et de spécifications en matière de sûreté préventive qui sont stratégiquement alignés au sein de l'entreprise.

4.2 Intégration

Les modalités de gouvernance servent de base à un programme de management de la sûreté qu'il convient d'intégrer à son tour dans les activités opérationnelles afin d'atteindre les objectifs de sûreté de l'organisme.

L'architecture de sûreté préventive de l'entreprise décrite dans le présent document comprend les principes, les modalités de gouvernance et les éléments structurels selon lesquels est mis en œuvre et géré le cadre des politiques, des processus et des spécifications en matière de sûreté préventive.

L'organisation du management de la sûreté selon ces axes nécessite le soutien de l'ensemble de l'organisme et un leadership fort de la part de la direction et des propriétaires d'actifs en particulier. De plus, étant donné qu'un management efficace des risques liés à la sûreté est essentiel pour obtenir des résultats en matière de sûreté, il convient que l'organisme mette en œuvre des processus de management du risque en cohérence avec l'ISO 31000:2018, Article 6 et s'assure que tous les éléments de gouvernance de la sûreté fonctionnent en accord avec l'ISO 31000 en général.

Il convient que les organismes identifient des normes techniques spécifiques en fonction des besoins ou, en l'absence de celles-ci, élaborent et mettent en œuvre des procédures sur la base des recommandations contenues dans le présent document et conformément aux meilleures pratiques nationales et internationales.

Il convient également d'aligner les contrôles non directement liés à la sûreté, mais qui peuvent atténuer ou accentuer le risque lié à la sûreté (gestion et réponse d'urgence, continuité d'activité, gestion de crise, sûreté et vie privée, par exemple) dans cette architecture de sûreté préventive de l'entreprise.

4.3 Éléments de l'architecture

Il convient que l'organisme mette en œuvre une architecture de sûreté préventive de l'entreprise comprenant les éléments spécifiés dans le Tableau 1.

Tableau 1 — Éléments de l'architecture de sûreté préventive de l'entreprise

Niveau		Description
1	Niveau de la gouvernance: Principes de sûreté préventive	Les principes qui régissent la stratégie, les objectifs, les ressources et la revue de la sûreté préventive au niveau du leadership et de la gouvernance de l'organisme.
2	Niveau managérial: Domaines de la sûreté préventive	Les domaines de pratique de la sûreté qui respectent ces principes directeurs en matière de sûreté des actifs de l'organisme.
3	Niveau de la mise en œuvre, des opérations et de la revue: Management des risques liés à la sûreté	Le management des risques liés à la sûreté permettant d'atteindre les objectifs de l'organisme. Des contrôles sont mis en œuvre pour atténuer/modifier/traiter le risque lié à la sûreté dans chacun des domaines de la sûreté: gouvernance de la sûreté, sûreté du personnel, sécurité de l'information, cybersécurité et sûreté physique. Une approche convergente garantit que l'application des contrôles est complémentaire aux résultats exigés en matière de sûreté. Des processus de mesure des performances et d'amélioration continue sont inclus à ce niveau.
	NOTE La surveillance des performances est développée en 6.2.2.7 et 6.2.2.8 et à l'Article 11.	

Les éléments de l'architecture de sûreté préventive de l'entreprise peuvent être étendus pour s'aligner sur le cadre plus détaillé des dispositifs de sûreté de l'organisme, tel que décrit à la Figure 1. L'existence de normes techniques pertinentes peut également faciliter l'application des traitements des risques. En l'absence de telles normes, il convient que l'organisme élabore et mette en œuvre des procédures sur la base du présent document.

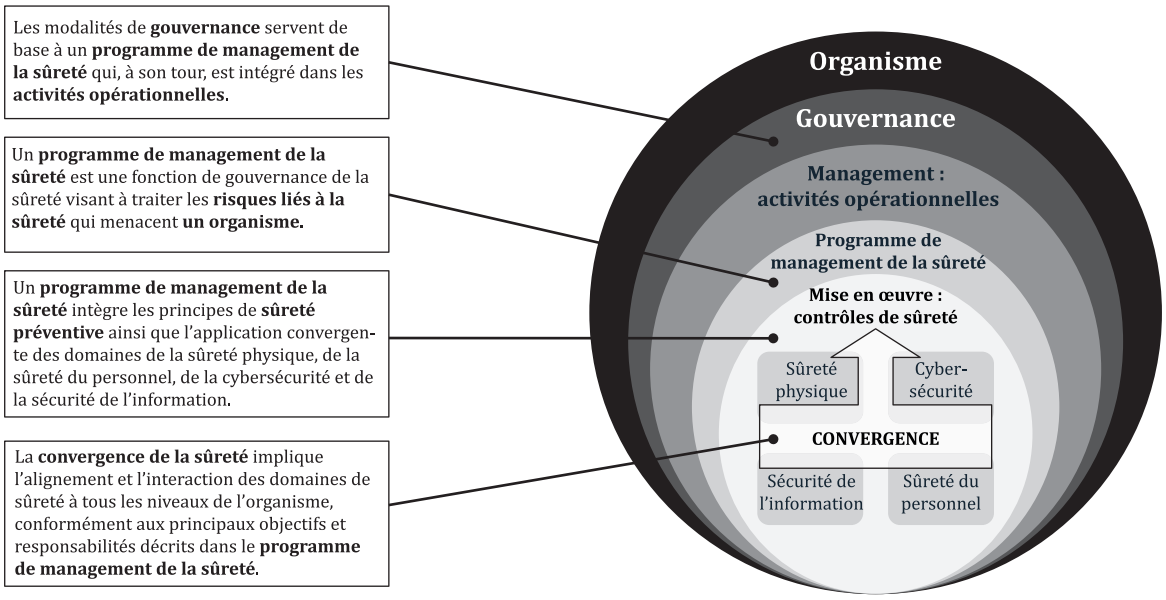

Figure 1 — Architecture étendue et vue du cadre

5 Principes et domaines de la sûreté préventive

5.1 Principes de sûreté préventive

Il convient que l'organisme soit guidé par les principes de sûreté préventive suivants lors de l'élaboration et de l'exécution des stratégies, politiques, procédures, processus et opérations de sûreté:

a) la sûreté est la responsabilité de tous: une culture positive, dans laquelle chacun a un rôle actif à jouer, est essentielle pour la sûreté;

b) la sûreté est au service de l'activité: la sûreté soutient la mission de l'organisme et la fourniture de ses produits et services;

c) le management de la sûreté repose sur les principes et la méthodologie de management du risque: les contrôles de sûreté sont appliqués de manière proportionnée pour protéger les actifs de l'organisme en fonction du risque global évalué par l'organisme;

NOTE 1 Un actif est un élément qui a de la valeur pour l'organisme, tel que les ressources humaines, matérielles, informationnelles, intangibles, environnementales et en matière d'infrastructure. Les actifs humains comprennent les employés, les sous-traitants ou d'autres parties intéressées. Les actifs ne doivent pas nécessairement appartenir à l'organisme.

d) la direction est comptable de la sûreté de l'organisme: la direction assume les risques de son organisme, investit dans la sûreté de l'organisme et la sponsorise, délègue les responsabilités en fonction des compétences et des ressources, et demande des comptes aux personnes à qui les responsabilités ont été déléguées;

e) la sûreté est intégrée à tous les niveaux d'activité de l'organisme: le risque lié à la sûreté est géré par des contrôles de sûreté préventive qui sont coordonnés dans l'ensemble de l'organisme;