NORME INTERNATIONALE

ISO 22396

Première édition
2020-02

Sécurité et résilience — Résilience des communautés — Lignes directrices pour l'échange d'informations entre les organismes

Security and resilience — Community resilience — Guidelines for information exchange between organizations

Numéro de référence
ISO 22396:2020(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **iv**
Introduction ..... **v**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Principes **2**
4.1 Généralités 2
4.2 Principes directeurs 2
5 Cadre **3**
5.1 Généralités 3
5.2 Responsabilité et engagement 3
5.3 Analyse du contexte 4
5.4 Conception et établissement d'un cadre 4
5.5 Mise en œuvre 4
5.6 Surveillance et revue 4
5.7 Amélioration continue 5
6 Processus **5**
6.1 Généralités 5
6.2 Établissement des besoins 6
6.2.1 Généralités 6
6.2.2 Déclaration d'intérêt 6
6.3 Préparation de chaque organisme 6
6.3.1 Interne 6
6.3.2 Externe 6
6.4 Définition de la structure d'échange d'informations 6
6.4.1 Généralités 6
6.4.2 Finalité 7
6.4.3 Lignes directrices d'adhésion 7
6.4.4 Système de classification des informations 7
6.5 Exploitation et maintien de l'échange d'informations 8
6.5.1 Généralités 8
6.5.2 Réunions 8
6.5.3 Plateforme de partage d'informations 8
6.5.4 Aspects techniques 9
6.6 Surveillance et revue 9
6.6.1 Généralités 9
6.6.2 Amélioration continue 9
Annexe A (informative) **Protocole d'échange d'information «Traffic Light Protocol» (protocole TLP)** **11**
Annexe B (informative) **Exemples** **12**
Bibliographie **14**

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 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 paysage des risques est en constante évolution pour tous les acteurs de la société, incluant les entreprises privées, les organismes gouvernementaux et les organismes non gouvernementaux. Les organismes sont devenus de plus en plus interconnectés et interdépendants, entraînant une accumulation des risques et leur expansion au-delà des frontières.

L'évolution des structures de propriété des infrastructures et services sociétaux essentiels signifie que les entreprises privées sont tenues de participer au développement de mécanismes visant à accroître la capacité d'adaptation, les expériences et les échanges de connaissances. Les infrastructures ou services sociétaux essentiels sont de plus en plus souvent gérés ou détenus par le secteur privé, ce qui crée de nouvelles exigences en matière de coopération et d'échange d'informations à des fins de renforcement des capacités.

Alors que les autorités ayant juridiction détiennent l'ultime responsabilité de servir et protéger leurs citoyens, des solutions émergent souvent dans le secteur privé, même si les actions préventives visant à augmenter la sécurité de fonctions sociétales essentielles sont traditionnellement perçues comme des domaines de compétence fondamentaux relevant du gouvernement et du secteur public. Aux fins d'améliorer et de promouvoir les actions préventives à visée protectrice, il convient que de multiples acteurs du secteur privé et du secteur public soient en mesure de s'échanger des informations de manière efficace et sécurisée afin d'accroître la sécurité sociétale et de renforcer la résilience.

De manière générale, l'objectif de cette collaboration est d'identifier et de mettre en place des actions visant à augmenter la sécurité et à réduire la vulnérabilité. L'échange d'informations sur les potentiels responsabilités, risques et vulnérabilités peut renforcer l'efficacité et l'efficience des organismes.

Il s'agit d'un objectif ambitieux, mais nécessaire à l'établissement de limites précises entre les organismes concernant le partage d'informations. La responsabilité en matière de coordination est également difficile à définir, car la coordination dans ces domaines exige des solutions spécifiques adaptées au sein d'un secteur pour chaque secteur, région ou nation différents.

Les acteurs du secteur privé exigent également une garantie que leurs informations commerciales sensibles ne seront pas divulguées, utilisées pour entraver la concurrence ou pour porter préjudice à leurs affaires ou à leur marque de commerce. Par conséquent, un échange d'informations sécurisé est une condition indispensable à un échange d'informations fructueux et efficace aussi bien pour les organismes du secteur public que du secteur privé.

Les organismes qui participent aux accords d'échange d'informations peuvent accroître leurs connaissances et leur compréhension des événements et des risques, avec l'objectif de renforcer leur résilience. Des accords d'échange d'informations peuvent offrir d'autres avantages aux organismes participants, notamment:

— en instruisant les organismes qui n'y ont généralement pas accès de la manière habituelle;

— en renforçant les capacités en autorisant l'accès à des informations sinon soumises à des restrictions;

— en créant un échange d'informations centralisé pour encourager le partage;

— en augmentant la capacité de diffusion des informations;

— en créant un sens de communauté par l'attention et le partage.

Le présent document se divise en trois sections: les principes, le cadre et le processus. Les principes constituent l'élément central du présent document. Le cadre identifie les éléments nécessaires au développement de cadres d'échange d'informations. Le processus décrit les procédures d'échange d'informations permettant d'établir et d'assurer le respect de l'accord. La Figure 1 illustre la relation entre les principes, le cadre et le processus.

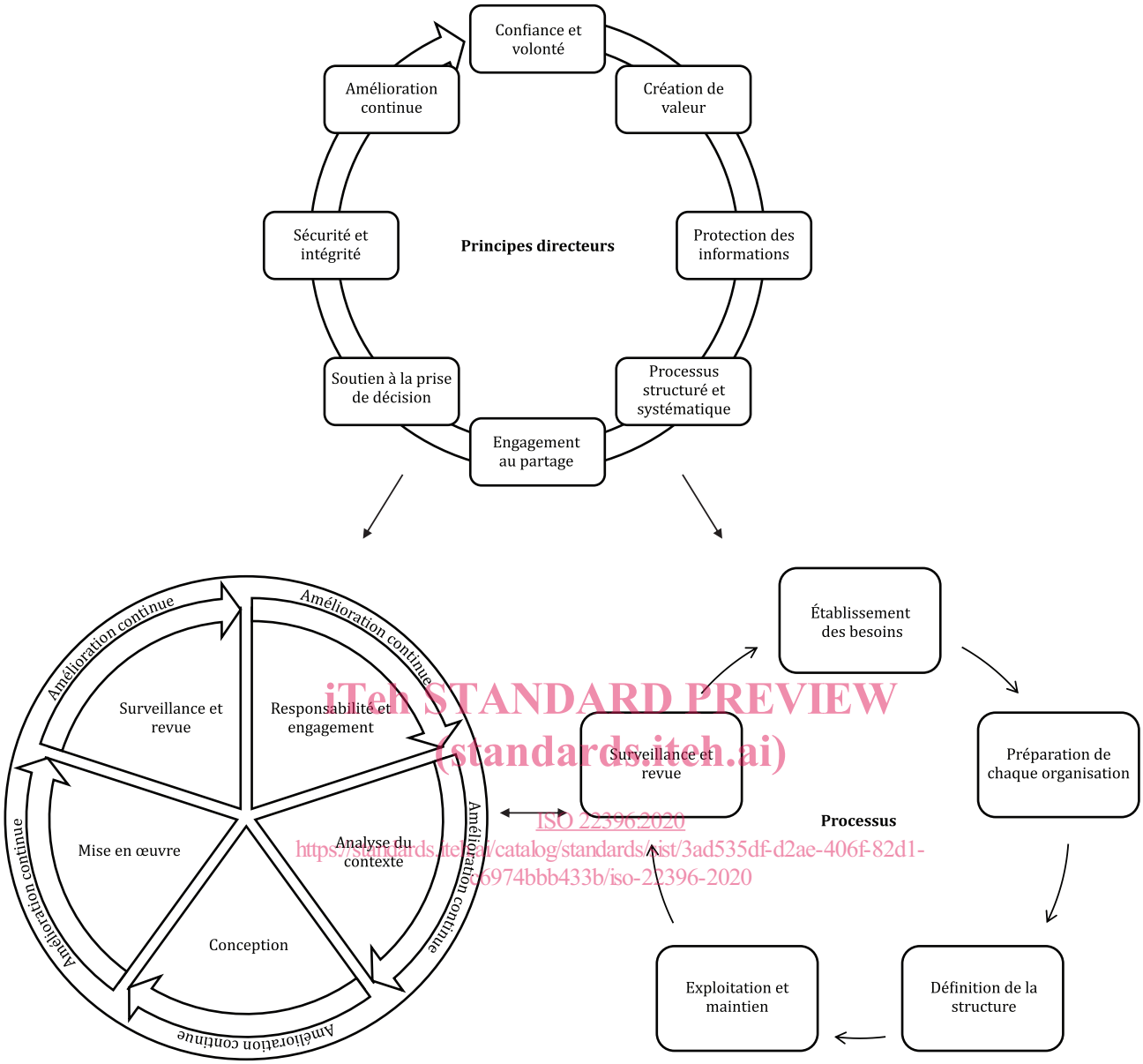

Figure 1 — Relation entre les principes, le cadre et le processus

Sécurité et résilience — Résilience des communautés — Lignes directrices pour l'échange d'informations entre les organismes

1 Domaine d'application

Le présent document fournit des lignes directrices pour l'échange d'informations. Il comporte des principes, un cadre et un processus applicables à l'échange d'informations. Il identifie des mécanismes d'échange d'informations qui permettent à un organisme participant d'apprendre des expériences, des erreurs et des succès des autres. Il peut être utilisé comme aide au respect de l'accord d'échange d'informations afin d'encourager la participation et l'engagement personnel. Il fournit des mesures qui renforcent la capacité des organismes participants à faire face au risque d'une perturbation.

Le présent document s'applique aux organismes privés et publics qui nécessitent des recommandations relatives à l'établissement de conditions propices à l'échange d'informations.

Le présent document ne s'applique pas aux aspects techniques, mais se concentre sur les problèmes de méthodologie.

NOTE La législation peut différer d'une juridiction à l'autre. Il appartient à l'utilisateur de déterminer la manière dont les exigences juridiques applicables se rapportent au présent document.

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 http://www.electropedia.org/

3.1
informations sensibles
informations devant être protégées de toute divulgation publique uniquement parce qu'elles auraient un effet négatif sur une personne, un organisme, la sécurité nationale ou la sécurité du public

[SOURCE: ISO 22300:2018, 3.244, modifiée — «une personne» a été ajouté.]

4 Principes

4.1 Généralités

L'objectif global de tout accord d'échange d'informations est de partager des informations entre des organismes de confiance dans le cadre d'une prise de décision éclairée aux fins d'accroître la sécurité et de renforcer la résilience (voir Annexe B pour des exemples). Bien que chaque accord d'échange soit unique, fondé sur les besoins et les ressources spécifiques des organismes participants, il convient que des principes communs servent de guides aussi bien à l'accord d'échange qu'à l'évaluation et à l'amélioration continue de l'échange, et ce dès le début.

4.2 Principes directeurs

Pour garantir un échange d'informations efficace, il convient que les organismes participants appliquent les principes directeurs suivants.

a) **Confiance et volonté**

L'échange d'informations repose sur la confiance et la volonté d'échanger des informations, y compris des informations sensibles.

b) **Création de valeur**

L'échange d'informations crée de la valeur, protège les valeurs acquises des organismes participants et se fonde sur un bénéfice mutuel.

c) **Protection des informations**

L'échange d'informations requiert une compréhension mutuelle des informations sensibles indiquées comme telles par chaque organisme participant.

d) **Processus structuré et systématique**

Les organismes qui partagent des informations le font dans le contexte de politiques, procédures et pratiques en matière d'information, des lois pertinentes et des principes de protection de la vie privée, et cet échange s'effectue dans un cadre systématique, pertinent et structuré.

e) **Engagement au partage**

L'échange d'informations se fonde sur un engagement à donner et à recevoir des informations dans le but de garantir une relation mutuellement avantageuse.

f) **Soutien à la prise de décision**

L'échange d'informations est utilisé pour soutenir la prise de décision et assister les opérations du quotidien.

g) **Sécurité et intégrité**

Des contrôles crédibles et efficaces de la sécurité et de l'intégrité garantissent l'efficacité des accords d'échange d'informations.

h) **Amélioration continue**

Les organismes participants s'engagent à mener des évaluations régulières afin d'identifier les opportunités d'amélioration continue de l'échange d'informations.

5 Cadre

5.1 Généralités

Le cadre garantit un échange d'informations efficace pour apporter des éléments de sens et de signification et éclairer la prise de décisions des organismes participants.

La Figure 2 décrit les composants du cadre à l'établissement et à la garantie du respect des accords d'échange d'informations.

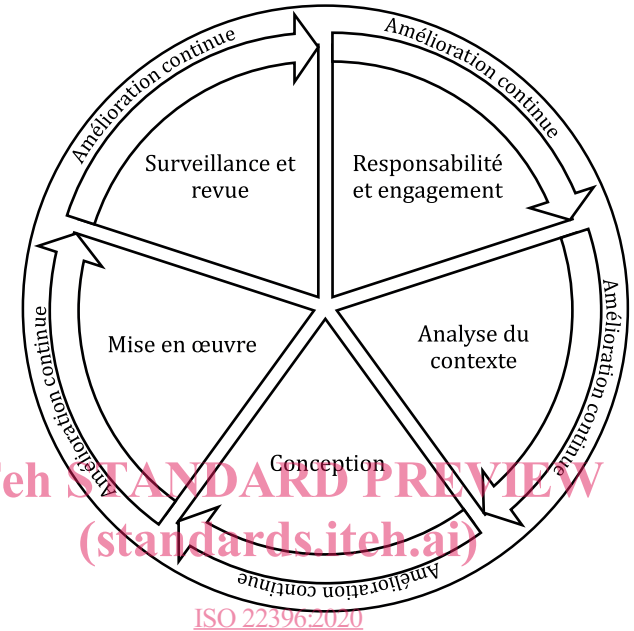

Figure 2 — Composants du cadre

5.2 Responsabilité et engagement

Il convient que la direction d'un organisme fasse preuve d'un engagement fort et soutenu afin de garantir l'efficacité continue de l'accord d'échange d'informations, en adaptant les composants du cadre et en soutenant l'accord dans la mesure nécessaire à la garantie de sa mise en œuvre efficace.

Il convient que la direction:

— définisse des objectifs pour l'échange d'informations dans le processus de création de valeur;

— définisse et adopte un cadre d'échange d'informations;

— garantisse l'engagement et la contribution de l'organisme;

— attribue les rôles et les responsabilités pour la participation;

— garantisse que les ressources nécessaires sont allouées à l'accord d'échange d'informations;

— communique les bénéfices du partage des informations dans le cadre de l'accord;

— détermine les critères de performance pour l'échange d'informations qui correspondent aux intérêts et au contexte des organismes participants;

— assure la conformité avec les politiques de son organisme;

— élabore un document d'orientation intégrant ces engagements.

5.3 Analyse du contexte

Avant de concevoir et de mettre en œuvre un cadre pour l'échange d'informations, il convient que les organismes participants évaluent et comprennent les contextes interne et externe qui auront un impact sur la conception.

L'évaluation du contexte externe des organismes participants peut comprendre:

— le contexte dans lequel il exerce ses activités;

— les principaux moteurs et tendances qui ont une influence sur le contexte;

— la relation avec leurs parties prenantes.

L'évaluation du contexte interne des organismes participants peut comprendre:

— l'identification des parties de chaque organisme qui doivent participer;

— l'identification des représentants de chaque organisme qui sont impliqués dans le processus.

5.4 Conception et établissement d'un cadre

Lors de la conception d'un cadre pour l'échange d'informations, il convient que la direction des organismes participants tienne compte:

— du modèle de gouvernance, de la structure organisationnelle, des rôles, des responsabilités et des principes pour la diffusion des informations;

— des capacités de ressource et des connaissances requises (par exemple, capital, temps, personnel, expertise);

— des processus formels et informels de prise de décision;

— des relations avec les parties prenantes internes ainsi que de leurs perceptions et de leurs valeurs;

— de la culture de l'organisme.

5.5 Mise en œuvre

Lors de la mise en œuvre du cadre, il convient que les organismes participants:

— communiquent et se concertent avec les parties prenantes afin de garantir que le cadre reste approprié;

— garantissent que la prise de décision, incluant l'élaboration et la définition d'objectifs, corresponde aux effets de l'accord d'échange d'informations.

5.6 Surveillance et revue

Afin de garantir un échange d'informations efficace et continu dans le but de soutenir la performance des organismes, il convient que les organismes participants:

— évaluent la réalisation des objectifs définis pour l'échange d'informations et les progrès accomplis par rapport à ceux-ci;

— procèdent à une revue de la documentation pour le processus d'échange d'informations (par exemple, plan de gestion des risques);

— procèdent à une revue du cadre;

— procèdent à une revue de la répartition des contributions des organismes participants.

Il convient que les organismes participants jouent un rôle de soutien auprès des autres organismes participants dans le cadre du processus de surveillance et de revue.

5.7 Amélioration continue

Il convient que les organismes participants utilisent les résultats du processus de surveillance et de revue pour améliorer en continu le cadre de l'échange d'informations.

Il convient que les enseignements tirés soient documentés et partagés entre les organismes participants.

6 Processus

6.1 Généralités

La Figure 3 représente un aperçu du processus d'échange d'informations.

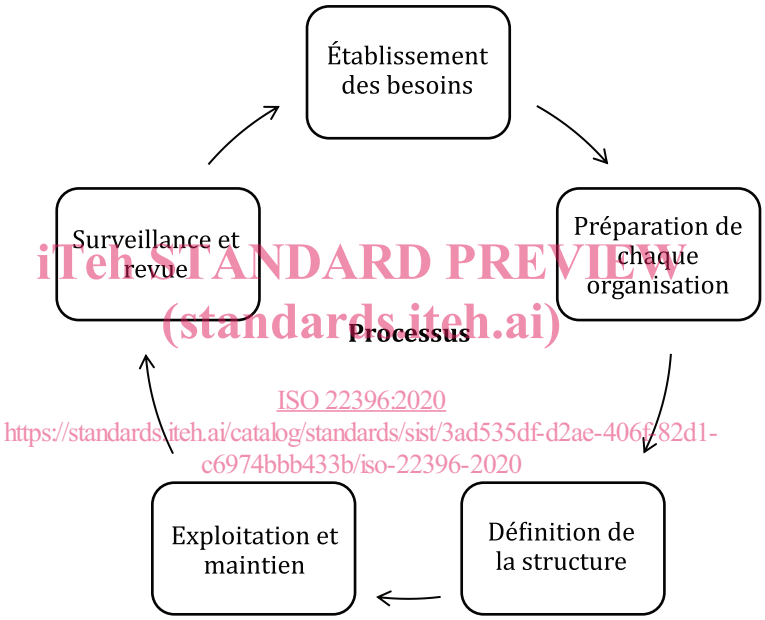

Figure 3 — Aperçu du processus d'échange d'informations

Il convient que les organismes participants:

— établissent et mettent en œuvre des accords d'échange d'informations en tant que mécanisme permettant à chaque organisme d'apprendre des suggestions, des expériences, des erreurs et des succès des autres;

— intègrent les accords d'échange d'informations dans les processus opérationnels globaux de chaque organisme;

— personnalisent et optimisent l'accord d'échange d'informations en fonction des exigences locales et du contexte de chaque organisme;

— s'assurent que les informations échangées font l'objet d'un processus garantissant la sécurité desdites informations.