NORME INTERNATIONALE

ISO 22313

Deuxième édition
2020-02

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices sur l'utilisation de l'ISO 22301

Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

Numéro de référence
ISO 22313:2020(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

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*.

Cette deuxième édition annule et remplace la première édition (ISO 22313:2012) qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

— modification de la structure et du contenu pour aligner le présent document sur la dernière édition de l'ISO 22301;

— ajout de lignes directrices supplémentaires expliquant les concepts et termes clés;

— suppression du contenu de 8.4, qui figurera dans l'ISO/TS 22332 (en cours d'élaboration).

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

0.1 Généralités

Le présent document fournit des lignes directrices, lorsque c'est opportun, applicables aux exigences spécifiées dans l'ISO 22301. Il n'est pas prévu que le présent document fournisse des lignes directrices sur tous les aspects de la continuité d'activité.

Le présent document comprend les mêmes rubriques que l'ISO 22301 sans toutefois répéter les exigences ou les termes et définitions qui s'y rapportent.

Ces lignes directrices ont pour vocation d'expliquer et de clarifier la signification et le but des exigences de l'ISO 22301 et d'aider à la résolution de tout problème lié à leur interprétation. D'autres Normes internationales et Spécifications techniques apportant des lignes directrices supplémentaires, et citées dans le présent document, sont l'ISO/TS 22317, l'ISO/TS 22318, l'ISO 22322, l'ISO/TS 22330, l'ISO/TS 22331 et l'ISO 22398. Le domaine d'application de ces documents peut s'étendre au-delà des exigences de l'ISO 22301. Il convient donc que les organismes fassent systématiquement référence à l'ISO 22301 afin de vérifier quelles exigences sont à satisfaire.

Le présent document comprend plusieurs figures permettant de donner des éclaircissements et des explications sur certains points clés. Ces figures ne sont fournies qu'à titre d'exemple, et c'est le texte associé faisant partie du corps du texte du présent document qui a la priorité.

Un système de management de la continuité d'activité (SMCA) insiste sur l'importance:

— d'établir une politique et des objectifs de de continuité d'activité qui correspondent aux objectifs de l'organisation;

— du fonctionnement et de la maintenance des processus, capacités et structures de réponse afin d'assurer que l'organisme survivra aux perturbations;

— de surveiller et passer en revue la performance et l'efficacité du SMCA;

— d'une amélioration continue sur la base de mesures qualitatives et quantitatives.

À l'instar de tout autre système de management, un SMCA comprend les composantes suivantes:

a) une politique;

b) des personnes compétentes ayant des responsabilités définies;

c) des processus de management concernant:

   1) la politique;

   2) la planification;

   3) la mise en œuvre et le fonctionnement;

   4) l'appréciation de la performance;

   5) la revue de direction;

   6) l'amélioration continue;

d) des informations documentées venant en support de la maîtrise opérationnelle et permettant de réaliser l'évaluation de la performance.

En général, la continuité d'activité est spécifique à un organisme. Néanmoins, sa mise en œuvre peut avoir des implications pouvant s'étendre à une plus large communauté et à d'autres tiers. Un organisme est susceptible d'avoir des organismes externes dont il dépend et d'autres qui dépendent de lui. Par conséquent, une continuité d'activité efficace contribue à une société plus résiliente.

0.2 Bénéfices d'un système de management de la continuité d'activité

Un SMCA améliore le niveau de préparation d'un organisme pour lui permettre de continuer à fonctionner pendant des perturbations. Il permet également une meilleure compréhension des relations internes et externes de l'organisme, une meilleure communication avec les parties intéressées, et la création d'un environnement d'amélioration continue. Il y a un grand nombre d'avantages potentiels supplémentaires à mettre en œuvre un SMCA conformément aux recommandations données dans le présent document et en conformité avec les exigences de l'ISO 22301.

— Le respect des recommandations de l'Article 4 («Contexte de l'organisme») appelle l'organisme:

  — à réviser ses objectifs stratégiques afin de s'assurer que le SMCA les supporte;

  — à reconsidérer les besoins, les attentes et les exigences des parties intéressées;

  — à avoir conscience des obligations réglementaires et juridiques, ainsi que des autres obligations applicables.

— L'Article 5 («Leadership») appelle l'organisme:

  — à reconsidérer les rôles et responsabilités du management;

  — à promouvoir une culture d'amélioration continue;

  — à répartir les responsabilités concernant la surveillance des performances et les rapports.

— L'Article 6 («Planification») appelle l'organisme:

  — à réexaminer ses risques et opportunités, et à identifier les actions à mener pour y faire face et en tirer parti;

  — à établir une gestion efficace des changements.

— L'Article 7 («Support») appelle l'organisme:

  — à établir une gestion efficace des ressources du SMCA, y compris la gestion des compétences;

  — à renforcer la sensibilisation (prise de conscience) des employés vis-à-vis de questions considérées comme importantes pour le management;

  — à disposer de mécanismes efficaces pour les communications internes et externes;

  — à gérer efficacement sa documentation.

— L'Article 8 («Fonctionnement») appelle l'organisme à considérer:

  — les conséquences imprévues du changement;

  — les priorités et exigences de continuité d'activité;

  — les dépendances;

  — les vulnérabilités du point de vue de leur impact;

  — les risques de perturbations et à identifier la meilleure manière d'y faire face;

  — les solutions alternatives pour poursuivre l'activité avec des ressources limitées;

  — les structures et procédures efficaces pour faire face aux perturbations;

— ses responsabilités envers la communauté et les autres parties intéressées.

— L'Article 9 («Évaluation de la performance») appelle l'organisme:

— à disposer de mécanismes efficaces de surveillance, de mesurage et d'évaluation de la performance;

— à impliquer le management pour surveiller la performance et contribuer à l'efficacité du SMCA.

— L'Article 10 («Amélioration») appelle l'organisme:

— à disposer de procédures de surveillance de la performance et d'amélioration de l'efficacité;

— à tirer parti de l'amélioration continue de ses systèmes de management.

En conséquence, la mise en œuvre du SMCA peut:

a) protéger la vie, les biens et l'environnement;

b) protéger et accroître la réputation et la crédibilité de l'organisme;

c) contribuer à l'avantage compétitif de l'organisme en lui permettant de fonctionner durant les perturbations;

d) réduire les coûts dus aux perturbations et améliorer la capacité de l'organisme à rester efficace durant ces perturbations;

e) contribuer à la résilience organisationnelle globale de l'organisme;

f) renforcer la confiance des parties intéressées en la réussite de l'organisme;

g) réduire l'exposition juridique et financière de l'organisme;

h) démontrer la capacité de l'organisme à gérer les risques et à faire face aux vulnérabilités opérationnelles.

0.3 Cycle «Planifier-Exécuter-Vérifier-Réagir» (Plan-Do-Check-Act, PDCA)

Le présent document applique le cycle «Planifier-Exécuter-Vérifier-Réagir» (PDCA) à la planification, l'établissement, la mise en œuvre, le fonctionnement, la surveillance, la revue, la maintenance et l'amélioration continue de l'efficacité du SMCA d'un organisme. Le cycle PDCA est expliqué dans le Tableau 1.

Tableau 1 — Explication du cycle PDCA

Planifier (Établir)	Établir une politique de continuité d'activité, des objectifs, des moyens de maîtrise, des processus et des procédures pertinents pour améliorer la continuité d'activité afin de fournir des résultats en ligne avec les politiques et objectifs généraux de l'organisme.
Exécuter (Mettre en œuvre et faire fonctionner)	Mettre en œuvre et faire fonctionner la politique de continuité d'activité, les moyens de maîtrise, les processus et les procédures.
Vérifier (Surveiller et passer en revue)	Surveiller et passer en revue la performance par rapport à la politique et aux objectifs de continuité d'activité, rendre compte des résultats au management pour la revue de direction, déterminer et autoriser des actions de correction et d'amélioration.
Réagir (Maintenir et améliorer)	Maintenir et améliorer le SMCA en prenant des actions correctives, basées sur les résultats de la revue de direction et en réévaluant le domaine d'application du SMCA, la politique et les objectifs de continuité d'activité.

La Figure 1 montre comment le SMCA prend les exigences des parties intéressées comme éléments d'entrée pour le management de la continuité d'activité et, par l'intermédiaire des actions et des processus requis, produit des résultats en matière de continuité d'activité (c'est-à-dire une continuité d'activité managée) qui satisfont à ces exigences.

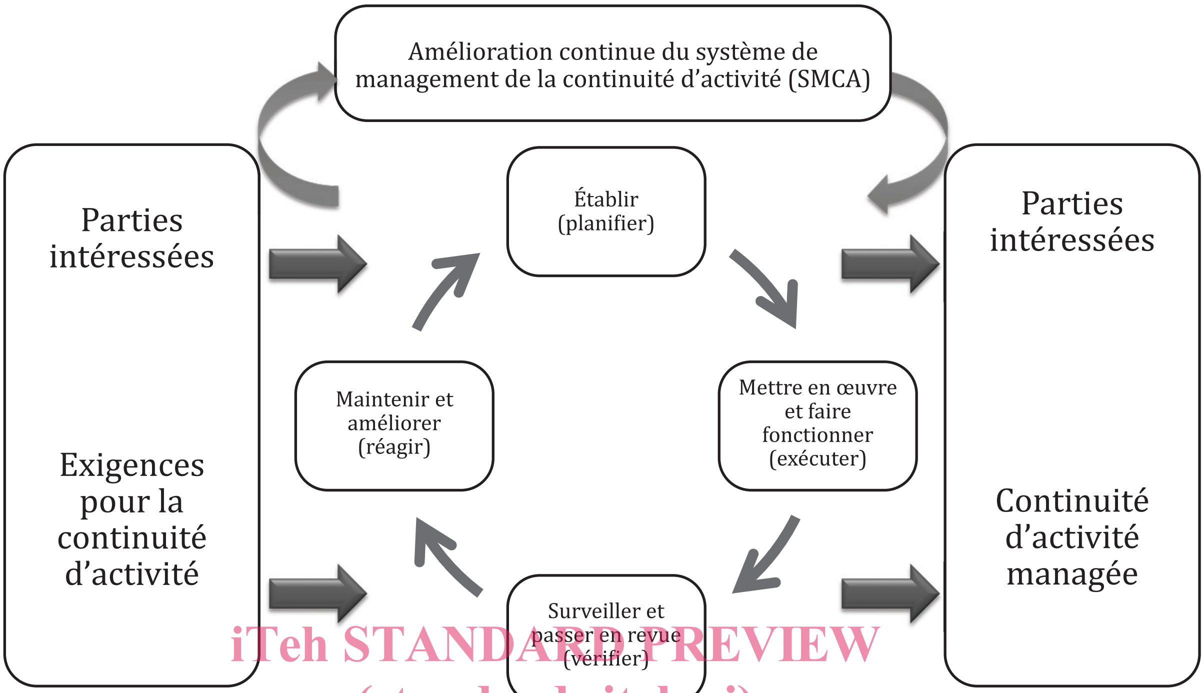

Figure 1 — Cycle PDCA appliqué aux processus SMCA

0.4 Composantes du cycle PDCA dans le présent document

Le Tableau 2 montre la relation directe entre le contenu de la Figure 1 et les articles du présent document.

Tableau 2 — Relation entre le cycle PDCA et les Articles 4 à 10

Composante PDCA	Article concernant la composante PDCA
Planifier (Établir)	L'Article 4 («Contexte de l'organisme») définit ce qu'il convient que l'organisme fasse afin d'assurer que le SMCA satisfait aux exigences, en tenant compte de tous les facteurs externes et internes pertinents, notamment: — les besoins et attentes des parties intéressées; — ses obligations réglementaires et juridiques; — le domaine d'application exigé pour le SMCA.
	L'Article 5 («Leadership») définit le rôle du management en matière de démonstration d'engagement, de définition de politique et d'établissement des rôles, responsabilités et autorités.
	L'Article 6 («Planification») décrit les actions pour établir des objectifs stratégiques et des principes d'orientation pour la mise en œuvre du SMCA.
	L'Article 7 («Support») identifie les éléments du SMCA dont il convient de disposer, à savoir: les ressources, les compétences, la sensibilisation (prise de conscience), la communication et les informations documentées.
Exécuter (Mettre en œuvre et faire fonctionner)	L'Article 8 («Fonctionnement») identifie les processus pour établir et maintenir la continuité d'activité.

Tableau 2 *(suite)*

Composante PDCA	Article concernant la composante PDCA
Vérifier (Surveiller et passer en revue)	L'Article 9 («Évaluation de la performance») donne la base pour améliorer le SMCA par le mesurage et pour évaluer sa performance.
Réagir (Maintenir et améliorer)	L'Article 10 («Amélioration») couvre les actions correctives pour faire face aux non-conformités identifiées par l'évaluation de la performance.

0.5 Contenu du présent document

Ce n'est pas l'intention du présent document d'uniformiser la structure d'un SMCA, mais plutôt de permettre à un organisme de concevoir un SMCA qui soit approprié à ses besoins et qui satisfasse aux exigences des parties intéressées, particulièrement les clients et les employés. Ces besoins sont conditionnés par les exigences réglementaires et juridiques, organisationnelles et industrielles, par les produits et services, les processus employés, l'environnement dans lequel l'organisme fonctionne, la taille et la structure de ce dernier et les exigences des parties intéressées.

Le présent document n'est pas destiné à être utilisé pour apprécier l'aptitude d'un organisme à satisfaire ses propres besoins de continuité d'activité, ni les besoins de clients ou de nature réglementaire ou juridique. Les organismes désireux de le faire peuvent utiliser les exigences de l'ISO 22301.

Les Articles 1 à 3 du présent document décrivent le domaine d'application, les références normatives et les termes et définitions qui s'appliquent à l'utilisation du présent document. Les Articles 4 à 10 donnent des lignes directrices relatives aux exigences de l'ISO 22301.

Dans le présent document, les formes verbales suivantes sont utilisées:

a) «il convient» est utilisé pour indiquer une recommandation;

b) «peut» («may» en anglais) est utilisé pour indiquer une autorisation;

c) «peut» («can» en anglais) est utilisé pour indiquer une possibilité ou une capacité.

0.6 Continuité d'activité

La continuité d'activité est la capacité de l'organisme à continuer de livrer des produits ou fournir des services avec un niveau prédéfini de capacité acceptable à la suite d'une perturbation. Le management de la continuité d'activité est le processus de mise en œuvre et de maintien de la continuité d'activité (voir 8.1.2 et Figure 5) afin de prévenir les pertes et de se préparer à des perturbations, de les atténuer et de les gérer.

L'établissement d'un SMCA permet à l'organisme de maîtriser, d'évaluer et de constamment améliorer sa continuité d'activité.

Dans le présent document, le terme «activité» est utilisé comme un terme de portée générale englobant les opérations et services accomplis par un organisme dans le cadre de ses objectifs, ses buts ou sa mission. Il s'applique à la fois aux grands, moyens et petits organismes fonctionnant dans les secteurs industriels, commerciaux, publics ou à but non lucratif.

Les perturbations peuvent potentiellement interrompre l'ensemble du fonctionnement de l'organisme ainsi que sa capacité à livrer des produits et fournir des services. Néanmoins, le fait de mettre en œuvre un SMCA avant qu'une perturbation ne se produise, plutôt que de répondre de manière non planifiée après l'incident, permettra à l'organisme de reprendre son fonctionnement avant d'en arriver à des niveaux d'impact inacceptables.

Le management de la continuité d'activité implique:

a) d'identifier les produits et services de l'organisme et les activités qui permettent de les fournir;

b) d'analyser les impacts d'une non-reprise des activités et les ressources dont ces dernières dépendent;

c) de comprendre le risque de perturbation;

d) de déterminer les priorités, délais, capacités et stratégies pour la reprise de la livraison des produits et de la fourniture des services;

e) d'avoir des solutions et des plans en place de façon à reprendre les activités dans les délais requis à la suite d'une perturbation;

f) de s'assurer que ces dispositions sont régulièrement passées en revue et mises à jour de manière à être efficaces en toutes circonstances.

Il convient que la démarche de l'organisme pour le management de la continuité d'activité et ses informations documentées soient appropriées à son contexte (par exemple: environnement opérationnel, complexité, besoins et ressources).

La continuité d'activité peut être efficace pour traiter à la fois les perturbations soudaines (telles que les explosions) et graduelles (telles que les pandémies).

Les activités peuvent être perturbées par une grande variété d'incidents, dont beaucoup sont difficiles à prévoir ou à analyser. En se concentrant sur l'impact de la perturbation plutôt que sur sa cause, la continuité d'activité permet à l'organisme d'identifier les activités essentielles pour pouvoir remplir ses obligations. Par la continuité d'activité, un organisme peut reconnaître ce qu'il est nécessaire de faire pour protéger ses ressources (par exemple: les personnes, les emplacements, la technologie et l'information), sa chaîne d'approvisionnement, les parties intéressées et sa réputation avant la survenance d'une perturbation. Ayant reconnu cela, l'organisme peut mettre en place une structure de réponse lui permettant de gérer les impacts d'une perturbation en confiance.

La Figure 2 et la Figure 3 illustrent conceptuellement la manière dont la continuité d'activité peut être efficace en atténuant les impacts dans certaines situations. La distance relative entre les différents stades représentés sur chacun des schémas ne représente aucune échelle de temps particulière.

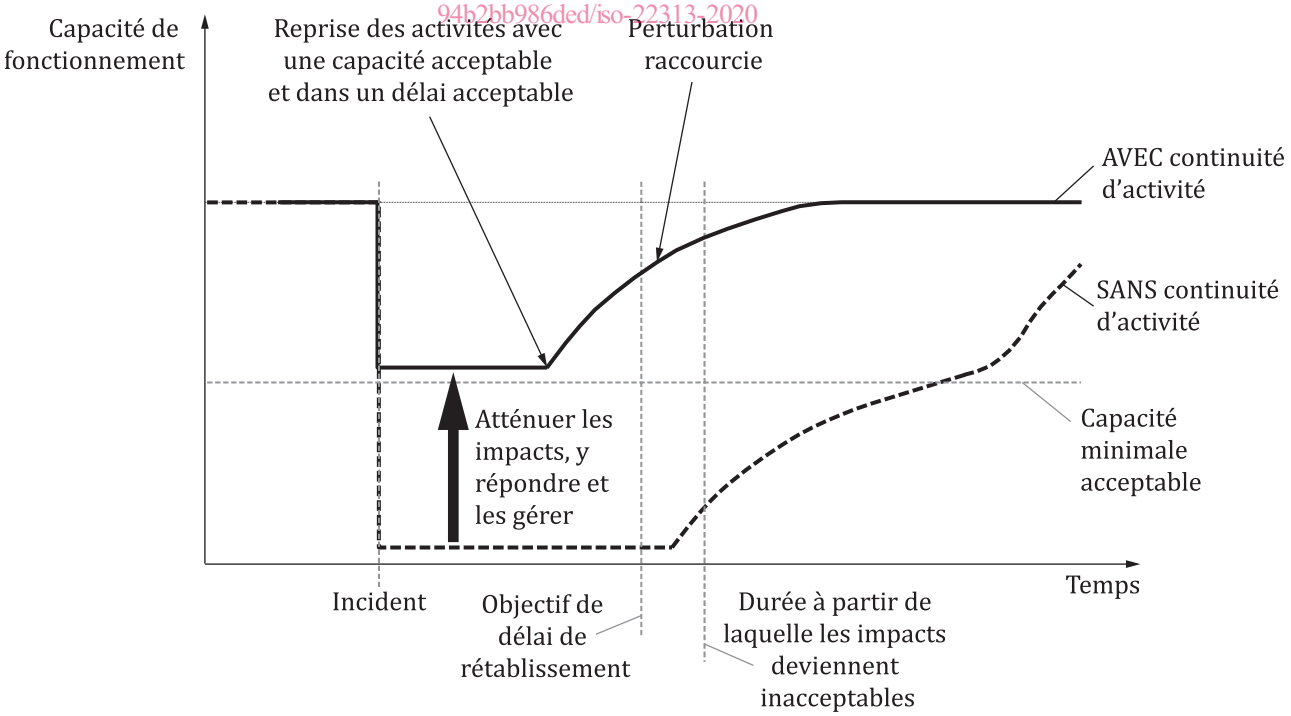

Figure 2 — Illustration de l'efficacité de la continuité d'activité en cas de perturbation soudaine

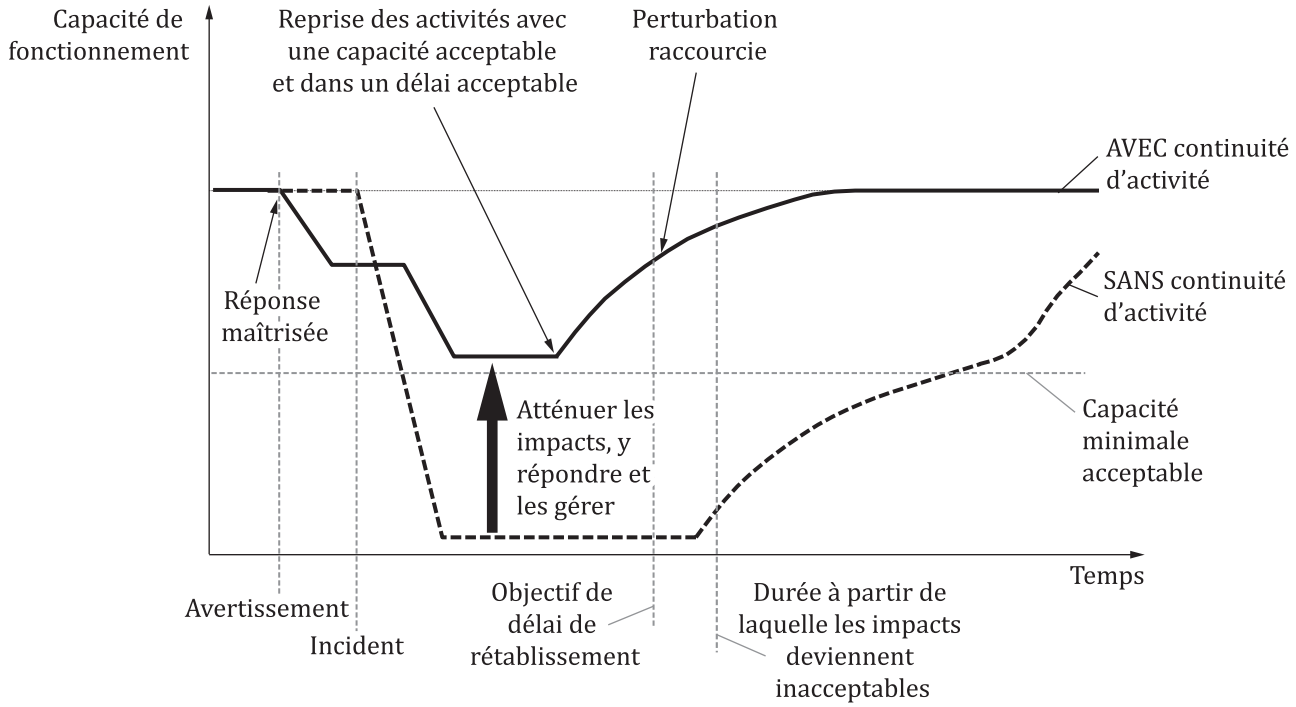

Figure 3 — Illustration de l'efficacité de la continuité d'activité en cas de perturbation graduelle (par exemple, l'approche d'une pandémie)

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices sur l'utilisation de l'ISO 22301

1 Domaine d'application

Le présent document donne des lignes directrices et recommandations relatives à l'application des exigences pour le système de management de la continuité d'activité (SMCA) de l'ISO 22301. Ces lignes directrices et recommandations sont basées sur la bonne pratique internationale.

Le présent document s'applique aux organismes qui:

a) mettent en œuvre, maintiennent et améliorent un SMCA;

b) cherchent à assurer la conformité à la politique de continuité d'activité déclarée;

c) ont besoin d'être aptes à poursuivre la livraison de produits et la fourniture de services à un niveau de capacité acceptable et préalablement défini durant une perturbation;

d) cherchent à améliorer leur résilience à travers l'application efficace du SMCA.

Les lignes directrices et recommandations s'appliquent à toute taille et tout type d'organismes, qu'ils soient grands, moyens ou petits et qu'ils fonctionnent dans les secteurs industriels, commerciaux, publics ou à but non lucratif. L'approche adoptée dépend de l'environnement et de la complexité de fonctionnement de l'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*

ISO 22301, *Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 22300, l'ISO 22301 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
management de la continuité d'activité
processus de mise en œuvre et de maintien de la continuité d'activité

4 Contexte de l'organisme

4.1 Compréhension de l'organisme et de son contexte

Le présent article fournit des recommandations pour la compréhension du contexte de l'organisme dans le cadre du SMCA. Les recommandations pour l'établissement et le maintien de la continuité d'activité sont traitées en 8.1.

Il convient que l'organisme évalue et comprenne les questions externes et internes (pouvant comprendre des facteurs positifs et négatifs ou des conditions à considérer) pertinentes pour ses objectifs globaux, pour ses produits et services, ainsi que pour le niveau et le type de risque qu'il peut prendre ou non. Il convient de tenir compte de ces informations lors de la mise en œuvre et de la maintenance du SMCA de l'organisme, et lors de l'attribution de priorités.

Le contexte externe de l'organisme contient, lorsque c'est pertinent, les éléments suivants:

— l'environnement politique, réglementaire et juridique, qu'il soit international, national, régional ou local;

— les aspects sociaux et culturels;

— l'environnement financier, technologique, économique, naturel et concurrentiel, qu'il soit international, national, régional ou local;

— les engagements et relations de la chaîne d'approvisionnement (voir également l'ISO/TS 22318);

— les moteurs (par exemple: risque, technologie) et tendances ayant un impact sur les objectifs et le fonctionnement de l'organisme;

— les relations avec les parties intéressées externes à l'organisme, ainsi que leurs perceptions et leurs valeurs;

— les voies de communication, y compris les réseaux sociaux, utilisées pour constater et former ces relations.

Le contexte interne de l'organisme contient, lorsque c'est pertinent, les éléments suivants:

— les produits et services, activités, ressources, chaînes d'approvisionnement et relations avec les parties intéressées;

— les aptitudes, en matière de ressources et de connaissances (par exemple: capital, temps, personnels, processus, systèmes, technologies);

— les systèmes de management existants;

— les informations et données (stockées sous forme physique ou électronique) et les processus de prise de décision (formels et autres);

— les parties intéressées au sein de l'organisme, y compris les fournisseurs internes [considération des accords sur les niveaux de services (SLA), résilience appréciée et dispositions de rétablissement], voir l'ISO/TS 22318;

— les politiques et objectifs et les stratégies d'activité mises en place pour les atteindre;

— les futures opportunités et priorités d'activité;

— les perceptions, les valeurs et la culture;

— les normes et modèles de référence adoptés par l'organisme;

— les structures (par exemple: gouvernance, rôles, responsabilités);

— les voies de communication internes utilisées pour l'échange d'informations au sein du personnel (par exemple: les réseaux sociaux).

4.2 Comprendre les besoins et attentes des parties intéressées

4.2.1 Généralités

L'organisme a un devoir de diligence envers de nombreuses personnes dans l'organisme et en dehors (voir également l'ISO/TS 22330). Lorsqu'il établit son SMCA, il convient que l'organisme s'assure que les besoins et les exigences de toutes les parties intéressées sont bien pris en considération.

Il convient que l'organisme identifie toutes les parties intéressées qui sont pertinentes pour son SMCA (voir Figure 4) et qu'il détermine leurs exigences sur la base de leurs besoins et attentes. Il est important d'identifier non seulement les exigences obligatoires et déclarées, mais aussi toutes celles qui sont implicites.

Lors de la planification et de la mise en œuvre du SMCA, il est important d'identifier les actions qui sont appropriées vis-à-vis des parties intéressées, mais aussi de les différencier entre elles. Par exemple, alors qu'il peut être approprié de communiquer avec toutes les parties intéressées à la suite d'une perturbation, il peut ne pas être approprié de communiquer avec toutes les parties intéressées lors de la mise en œuvre et de la maintenance du management de la continuité d'activité (voir 8.1.2).

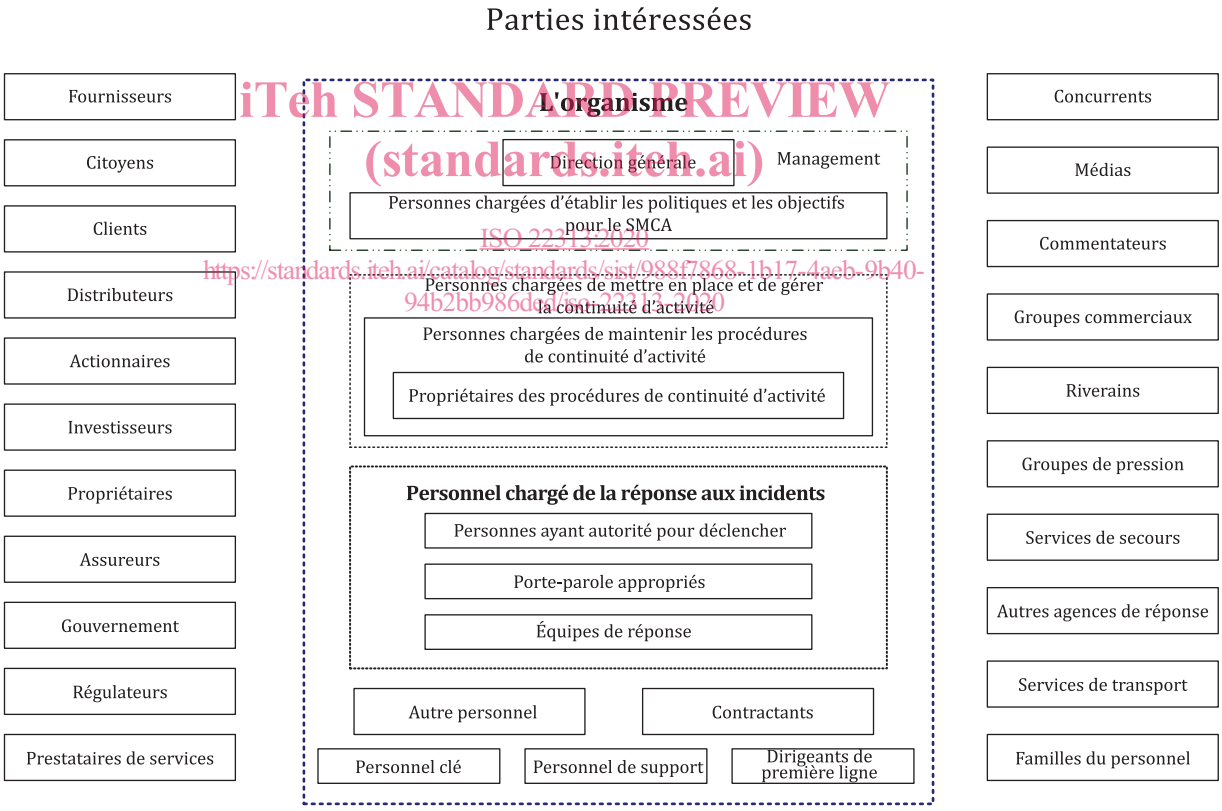

Figure 4 — Exemples de parties intéressées dans les secteurs public et privé

4.2.2 Exigences réglementaires et juridiques

L'application du présent document présuppose une sensibilisation (prise de conscience) aux exigences réglementaires et juridiques applicables.

Les exigences peuvent être implicites, déclarées ou obligatoires. Il convient que les informations relatives à ces exigences soient documentées et maintenues à jour. Il convient que les nouvelles