ICS: 03.100.01

norme belge enregistrée

NBN ISO 22313

1e éd., septembre 2014

Indice de classement: X 04

Sécurité sociétale - Systèmes de management de la continuité d'activité - Lignes directrices (ISO 22313:2012)

Maatschappelijke veiligheid - Business continuity managementsystemen - Leidraad (ISO 22313:2012)

Societal security - Business continuity management systems - Guidance (ISO 22313:2012)

Autorisation de publication: 26 septembre 2014

La présente norme ISO 22313:2014 a le statut d'une norme belge.

La présente norme existe en deux versions officielles (anglais, français).

standards for .be

Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique

Tél: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be

Banque 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB TVA BE0880857592

Prix: groupe 33

ICS: 03.100.01

Geregistreerde Belgische norm

NBN ISO 22313

1e uitg., september 2014

Normklasse: X 04

Maatschappelijke veiligheid - Business continuity managementsystemen - Leidraad (ISO 22313:2012)

Sécurité sociétale - Systèmes de management de la continuité d'activité - Lignes directrices (ISO 22313:2012)

Societal security - Business continuity management systems - Guidance (ISO 22313:2012)

Toelating tot publicatie: 26 september 2014

Deze norm ISO 22313:2014 heeft de status van een Belgische norm.

Deze norm bestaat in twee officiële versies (Engels, Frans).

standards for .be

Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België

Tel: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be

Bank 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB BTW BE0880857592

Prijsgroep: 33

NBN ISO 22313 (2014)

NORME INTERNATIONALE

ISO 22313

Première édition
2012-12-15

Sécurité sociétale — Systèmes de management de la continuité d'activité — Lignes directrices

Societal security — Business continuity management systems — Guidance

Numéro de référence
ISO 22313:2012(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2014

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 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. 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 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'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires.

Le comité chargé de l'élaboration du présent document est l'ISO/TC 223, *Sécurité sociétale*.

Introduction

Généralités

La présente Norme internationale fournit des lignes directrices, lorsque c'est opportun, applicables aux exigences spécifiées dans l'ISO 22301:2012 et donne des recommandations (« il convient de ») et des permissions (« peut ») en lien avec ces exigences. Il n'est pas prévu que la présente Norme internationale fournisse des lignes directrices sur tous les aspects de la continuité d'activité.

La présente Norme internationale comprend les mêmes rubriques que l'ISO 22301, sans toutefois répéter les exigences applicables aux systèmes de management de la continuité d'activité, ni ses termes et définitions qui s'y rapportent. Les organisations souhaitant s'informer à ce sujet doivent par conséquent se reporter aux normes ISO 22301 et ISO 22300.

La présente Norme internationale comprend un certain nombre de données permettant de donner des éclaircissements et des explications sur certains points clés. Toutes ces données ne sont fournies qu'à titre d'exemple et c'est le texte associé faisant partie du corps du texte de la présente Norme internationale qui a la priorité.

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

— de comprendre les besoins de l'organisation et la nécessité de définir une politique et des objectifs de continuité d'activité;

— de mettre en place et d'employer des contrôles et des moyens de management de la capacité d'ensemble d'une organisation à gérer les incidents perturbateurs;

— de surveiller et passer en revue les performances et l'efficacité du SMCA;

— d'améliorer en continu les processus sur la base de mesures objectives.

À l'instar de tout autre système de management, un SMCA comprend les composants essentiels suivants:

a) une politique;

b) des personnes 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'évaluation des performances;

   5) la revue de direction;

   6) les actions d'amélioration.

d) une documentation constituant une preuve vérifiable;

e) tout processus SMCA important pour l'organisation.

En général, la continuité d'activité est spécifique à une organisation. Néanmoins, sa mise en œuvre peut avoir des implications pouvant s'étendre à la collectivité et à des tiers. Une organisation tend à avoir des organisations externes dont elle dépend, tandis que d'autres dépendent d'elle. Par conséquent, une continuité d'activité efficace contribue à renforcer la solidité d'une société.

Le cycle «Planifier-Déployer-Contrôler-Agir»

La présente Norme internationale applique le cycle «Planifier-Déployer-Contrôler-Agir» (PDCA) pour planifier, définir, mettre en œuvre, exécuter, surveiller, réexaminer, mettre à jour et améliorer en continu l'efficacité du SMCA d'une organisation.

La Figure 1 montre comment le SMCA prend les exigences des parties prenantes comme données d'entrée pour le management de la continuité d'activité (MCA) et, par l'intermédiaire des actions requises et des processus, produit des résultats en matière de continuité d'activité (c'est-à-dire une continuité d'activité gérée) dans le respect de ces exigences.

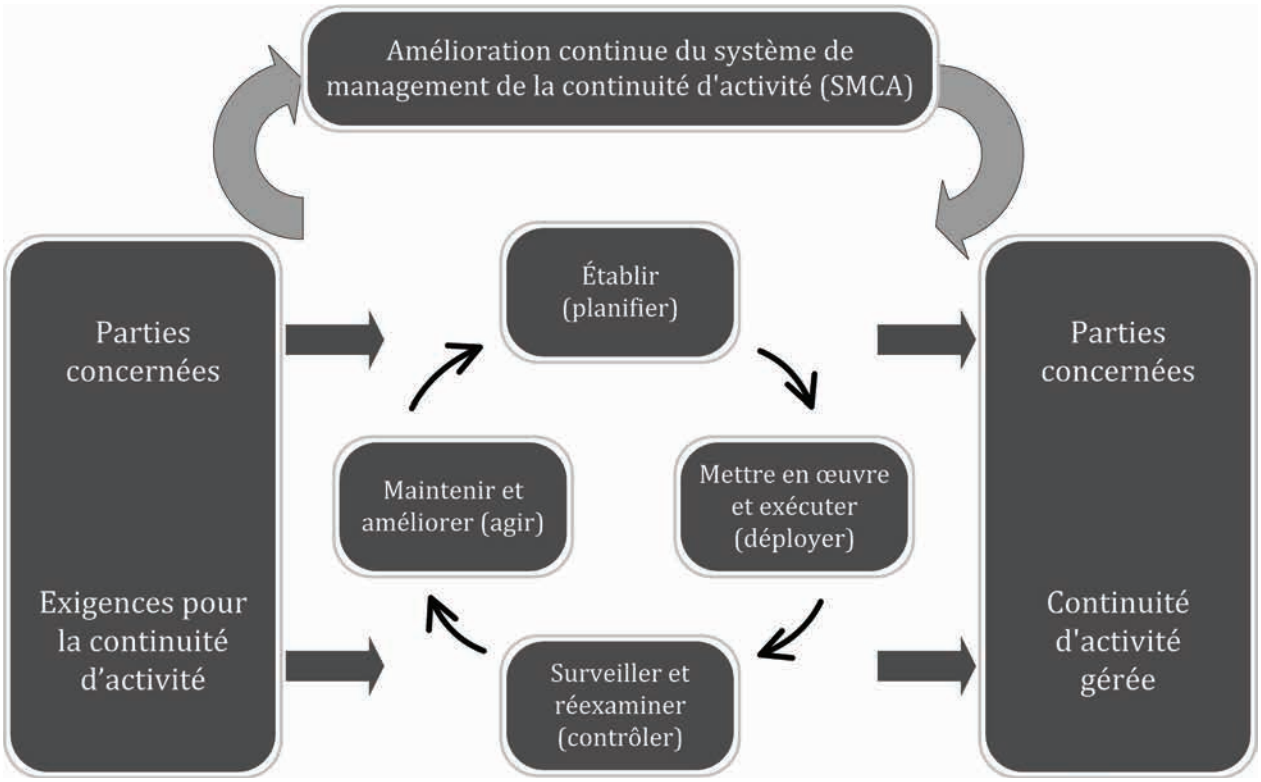

Figure 1 — Modèle PDCA appliqué aux processus SMCA

Tableau 1 — Explication du modèle PDCA

Planifier (établir)	Établir une politique de continuité d'activité, des objectifs, des contrôles, des processus et des procédures importants pour améliorer la continuité d'activité afin de fournir des résultats en accord avec les politiques et objectifs généraux de l'organisation.
Déployer (Mettre en œuvre et exécuter)	Mettre en œuvre et exécuter la politique de continuité d'activité, les contrôles, processus et procédures.
Contrôler (surveiller et réexaminer)	Surveiller et réexaminer les performances par rapport à des objectifs et à une politique de continuité d'activité, rendre compte des résultats au management pour examen, déterminer et autoriser des actions de correction et d'amélioration.
Agir (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 l'objet du SMCA et de la politique et des objectifs de continuité d'activité.

Les composants du cycle PDCA dans la présente Norme internationale

Il existe une relation directe entre le contenu de la Figure 1 et les articles de la présente Norme internationale.

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

Composante PDCA	Article concernant la composante PDCA
Planifier (établir)	L'Article 4 **(Contexte de l'organisation)** définit ce que l'organisation doit faire afin de s'assurer que le SMCA répond à ses exigences, en tenant compte de tous les facteurs externes et internes concernés, notamment:
	– les besoins et les attentes des parties intéressées;
	– ses obligations légales et réglementaires;
	– le périmètre d'application voulu du SMCA.
	L'Article 5 **(Leadership)** définit le rôle clé du management en termes de démonstration d'engagement, de définition de politique et d'établissement des rôles, responsabilités et autorités.
	L'Article 6 **(Planification)** décrit les actions nécessaires pour établir des objectifs stratégiques et des principes d'orientation pour le SMCA dans sa globalité. Celles-ci définissent le contexte de l'analyse d'impact sur les affaires et de l'évaluation des risques (8.2), ainsi que la stratégie de continuité d'activité (8.3).
	L'Article 7 **(Appui)** identifie les éléments clés devant être en place pour appuyer le SMCA, à savoir: les ressources, la compétence, la sensibilisation, la communication et des informations documentées.
Déployer (Mettre en œuvre et exécuter)	L'Article 8 **(Exécution)** identifie les éléments de management de la continuité d'activité (MCA) nécessaires pour assurer la continuité d'activité.
Contrôler (surveiller et réexaminer)	L'Article 9 **(Évaluation des performances)** donne la base de l'amélioration du SMCA par la mesure et l'évaluation de ses performances.
Agir (Maintenir et améliorer)	L'Article 10 **(Amélioration)** couvre les actions correctives nécessaires pour résoudre les non-conformités identifiées par l'évaluation des performances.

Continuité d'activité

La continuité d'activité est la capacité de l'organisation à continuer de livrer des produits ou des services à des niveaux acceptables prédéfinis à la suite d'un incident perturbateur. Le management de la continuité d'activité (MCA) est le processus assurant la continuité d'activité. Il consiste à préparer une organisation à gérer les incidents perturbateurs qui, autrement, seraient susceptibles de l'empêcher d'atteindre ses objectifs.

Le fait de placer le MCA dans le cadre et parmi les disciplines propres à un système de management crée un système de management de la continuité d'activité (SMCA) permettant au MCA d'être contrôlée, évaluée et constamment améliorée.

Dans la présente Norme internationale, le terme «affaires» est utilisé dans toutes les acceptions du terme applicables aux opérations et services accomplis par une organisation dans la poursuite de ses objectifs, buts ou mission. Il s'applique également aux grandes, moyennes et petites organisations intervenant dans les secteurs industriels, commerciaux, publics et à but non lucratif.

Tout incident, grand ou petit, naturel, accidentel ou délibéré est susceptible de provoquer une perturbation majeure sur le fonctionnement de l'organisation et sur son aptitude à livrer des produits ou des services. Néanmoins, le fait de mettre en place une continuité d'activité avant qu'un incident perturbateur ne se produise, plutôt que d'attendre qu'il arrive, permettra à l'organisation de reprendre son fonctionnement avant d'en arriver à des niveaux d'impact inacceptables.

Le SMCA implique:

a) d'être bien clair sur les produits et services clés de l'organisation et sur les activités qui permettent de les livrer;

b) de connaître les priorités pour la reprise des activités et les ressources que cela exige;

c) d'avoir une bonne compréhension des menaces pour ces activités, notamment de leurs dépendances, et de connaître les impacts d'une absence de reprise;

d) d'avoir mis en place des dispositions ayant été testées et fiables pour reprendre ces activités à la suite d'un incident perturbateur;

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

La continuité d'activité peut être efficace pour traiter à la fois les incidents perturbateurs soudains (tels que les explosions) et graduels (tels que les pandémies de grippe).

Les activités sont perturbées par une large variété d'incidents, dont la plupart sont difficiles à prévoir ou à analyser. En mettant l'accent sur l'impact de la perturbation plutôt que sur sa cause, la continuité d'activité identifie les activités desquelles l'organisation dépend pour sa survie, et permet à l'organisation de déterminer ce qu'il lui faut pour continuer de remplir ses obligations. Par la continuité d'activité, une organisation peut reconnaître ce qui doit être fait pour protéger ses ressources (par exemple les personnes, les locaux, la technologie et l'information), sa chaîne d'approvisionnement, les parties prenantes et sa réputation avant la survenance d'un incident perturbateur. Ayant reconnu cela, l'organisation est en mesure d'avoir une vision réaliste des réponses qui seront probablement nécessaires lorsqu'un incident surviendra, afin d'être confiante dans la gestion des conséquences et d'éviter les impacts inacceptables.

Une organisation avec une continuité d'activité appropriée en place peut également profiter d'opportunités qui, autrement, pourraient être considérées comme trop risquées.

Les schémas suivants (Figures 2 et 3) ont pour but d'illustrer conceptuellement la manière dont la continuité d'activité peut être efficace en réduisant les impacts dans certaines situations. La distance relative entre les différents stades représentés sur chacun des schémas ne représente aucune échelle de temps particulière.

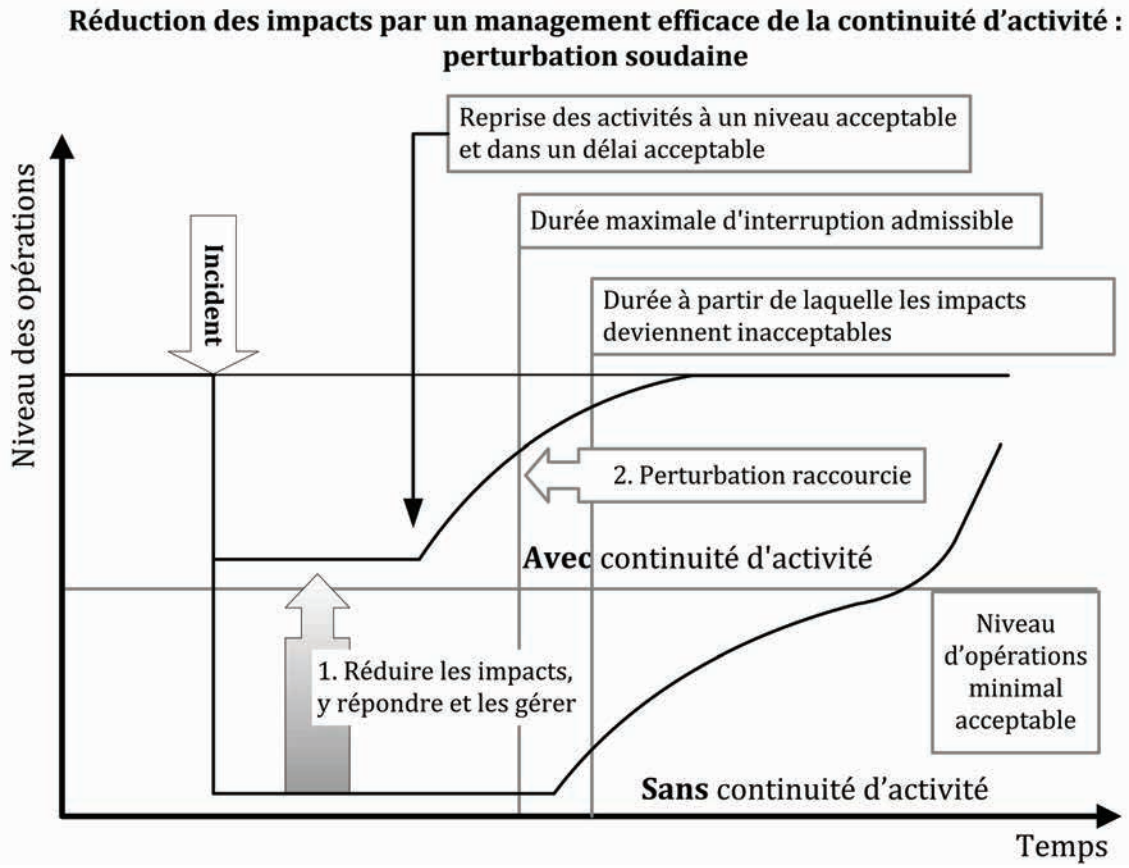

Figure 2 — Illustration de l'efficacité de la continuité d'activité en cas de perturbation soudaine

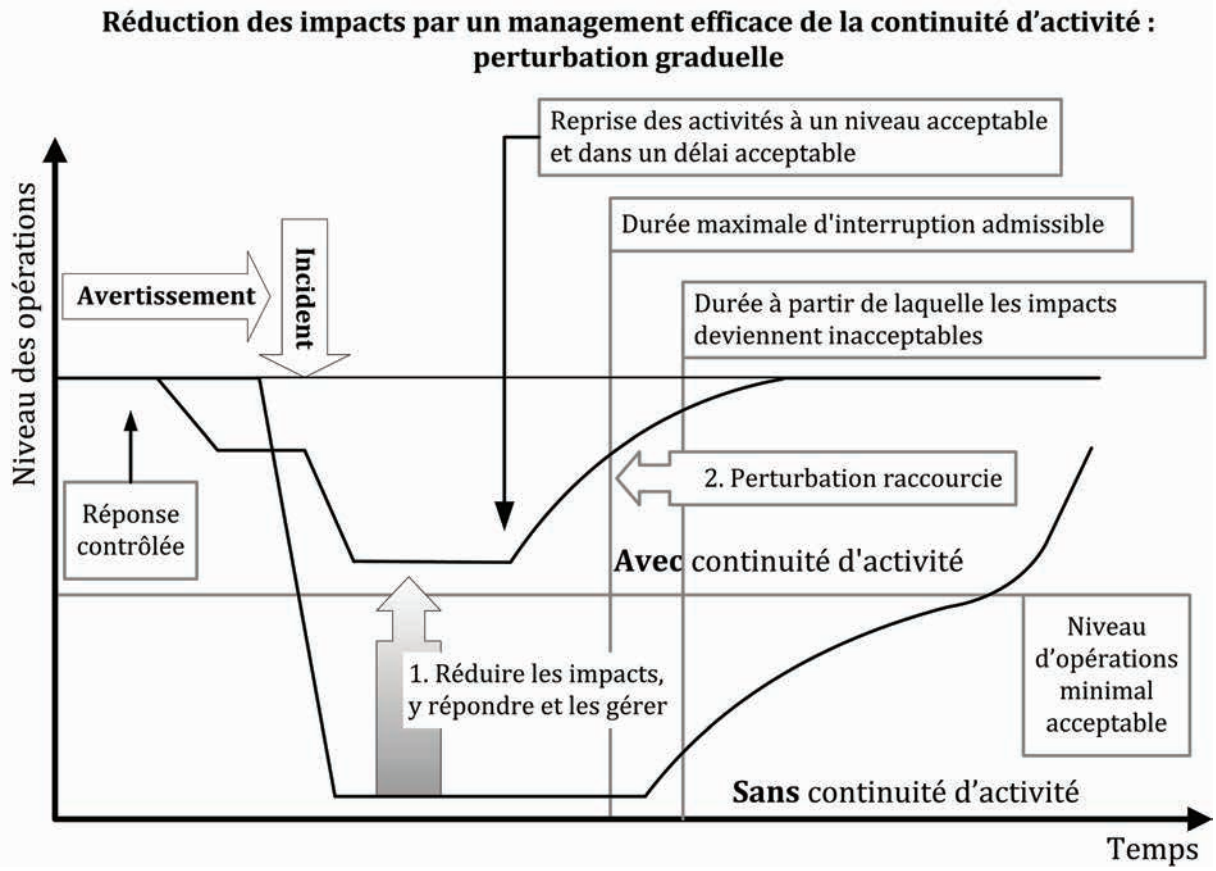

Figure 3 — Illustration de l'efficacité de la continuité d'activité en cas de perturbation graduelle (par exemple, l'approche d'une pandémie)

NORME INTERNATIONALE **ISO 22313:2012(F)**

Sécurité sociétale — Systèmes de management de la continuité d'activité — Lignes directrices

1 Domaine d'application

La présente Norme internationale relative aux systèmes de management de la continuité d'activité fournit des lignes directrices basées sur une bonne pratique internationale pour la planification, l'établissement, la mise en œuvre, l'exploitation, la surveillance, le réexamen, la mise à jour et l'amélioration constante d'un système de management documenté permettant aux organisations de se préparer aux incidents perturbateurs, d'y répondre et de reprendre leurs activités lorsqu'ils surviennent.

La présente Norme internationale ne prétend pas uniformiser la structure d'un SMCA, mais permettre à une organisation de définir un SMCA qui convienne à ses besoins et qui réponde aux exigences des parties concernées. Ces besoins sont conditionnés par les exigences légales, réglementaires, organisationnelles et industrielles, par les produits et les services, les processus employés, l'environnement dans lequel l'organisation fonctionne, la taille et la structure de cette dernière et les exigences des parties concernées.

La présente Norme internationale est générique et s'applique à toute taille et tout type d'organisations, qu'elles soient grandes, moyennes ou petites et qu'elles interviennent dans les secteurs industriels, commerciaux, publics et à but non lucratif, dans la mesure où elles souhaitent:

a) établir, mettre en œuvre, maintenir et améliorer un SMCA;

b) assurer la conformité avec la politique de continuité d'activité de l'organisation;

c) procéder à une autodétermination et effectuer une auto-déclaration de conformité avec la présente Norme internationale.

La présente Norme internationale ne peut pas servir à évaluer l'aptitude d'une organisation à satisfaire ses propres besoins de continuité d'activité, ni ses besoins commerciaux, légaux ou réglementaires. Les organisations désireuses de le faire peuvent utiliser les exigences de l'ISO 22301 pour démontrer leur conformité vis-à-vis d'autres exigences ou solliciter une certification de leur SMCA auprès d'un organisme tiers de certification accrédité.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application 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 sociétale — Terminologie.*

ISO 22301, *Sécurité sociétale — Systèmes de management de la continuité d'activité — Exigences.*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 22300 et l'ISO 22301 s'appliquent.