Norme belge

ISO 22301:2019
EN ISO 22301:2019
NBN EN ISO 22301:2019

Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2019)

Valable à partir de 28-11-2019

Remplace NBN EN ISO 22301:2014

ICS: 03.100.01, 03.100.70

Bureau de Normalisation
Rue Joseph-II 40 bte 6
1000 Bruxelles

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

NORME EUROPÉENNE

EUROPÄISCHE NORM

EUROPEAN STANDARD

EN ISO 22301

Novembre 2019

ICS 03.100.01; 03.100.70

Remplace l' EN ISO 22301:2014

Version Française

Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2019)

Sicherheit und Resilienz - Business Continuity Management System - Anforderungen (ISO 22301:2019)

Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019)

La présente Norme européenne a été adoptée par le CEN le 14 octobre 2019.

Les membres du CEN sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN sont les organismes nationaux de normalisation des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Bruxelles

Réf. n° EN ISO 22301:2019 F

EN ISO 22301:2019 (F)

Sommaire

Page

Avant-propos européen

Le présent document (EN ISO 22301:2019) a été élaboré par le Comité Technique ISO/TC 292 « Sécurité et résilience » en collaboration avec le Comité Technique CEN/TC 391 « Sécurité sociétale et citoyenne » dont le secrétariat est tenu par AFNOR.

La présente Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en mai 2020 et les normes nationales en contradiction devront être retirées au plus tard en mai 2020.

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. Le CEN ne saurait être tenu responsable de l'identification de tels ou tels brevets.

Ce document remplace l'EN ISO 22301:2014.

Selon le règlement intérieur du CEN/CENELEC, les instituts de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Notice d'entérinement

Le texte de l'ISO 22301:2019 a été approuvé par le CEN comme EN ISO 22301:2019 sans aucune modification.

NORME INTERNATIONALE

ISO 22301

Deuxième édition
2019-10

Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences

Security and resilience — Business continuity management systems — Requirements

Numéro de référence
ISO 22301:2019(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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 22301:2012), qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

— application des exigences de l'ISO en matière de normes de système de management, qui ont évolué depuis 2012;

— clarification des exigences, sans ajout de nouvelles exigences;

— inclusion dans l'Article 8 de la quasi-totalité des exigences de continuité d'activité en lien avec des disciplines spécifiques;

— restructuration de l'Article 8 pour faciliter la compréhension des exigences essentielles;

— modification d'un certain nombre de termes relatifs à la continuité d'activité en lien avec des disciplines spécifiques pour en améliorer la clarté et refléter les pensées actuelles.

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 spécifie la structure et les exigences relatives à la mise en œuvre et à la maintenance d'un Système de Management de la Continuité d'Activité (SMCA) qui développe une continuité d'activité en fonction de l'importance et du type d'impact que l'organisme peut ou non accepter suite à une perturbation.

Les résultats de la maintenance d'un SMCA sont façonnés par les exigences réglementaires, juridiques, organisationnelles et sectorielles de l'organisme, les produits et services offerts, les processus employés, la taille et la structure de l'organisme et les exigences de ses parties intéressées.

Un SMCA souligne l'importance:

— d'une compréhension des besoins de l'organisme et de la nécessité d'établir des politiques et des objectifs de continuité d'activité;

— 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 des performances;

   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.

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

Un SMCA sert à préparer, fournir et maintenir les moyens de maîtrise et les capacités pour gérer l'aptitude globale d'un organisme à continuer à fonctionner pendant les perturbations. En atteignant ce but, l'organisme:

a) du point de vue de l'activité métier:

   1) contribue à ses objectifs stratégiques;

   2) acquiert un avantage concurrentiel;

   3) protège et renforce sa réputation et sa crédibilité;

4) contribue à la résilience de l'organisme;

b) d'un point de vue financier:

1) réduit l'exposition juridique et financière;

2) diminue les coûts directs et indirects des perturbations;

c) du point de vue des parties intéressées:

1) protège la vie, la propriété et l'environnement;

2) prend en considération les attentes des parties intéressées;

3) renforce leur confiance en sa capacité de réussite;

d) du point de vue des processus internes:

1) améliore sa capacité à rester efficace pendant les perturbations;

2) démontre une maîtrise proactive des risques de façon efficace et efficiente;

3) traite les vulnérabilités opérationnelles.

0.3 Cycle PDCA (Plan-Do-Check-Act/Planifier–Déployer–Contrôler-Agir)

Le présent document applique le cycle PDCA [Planifier (établir), Déployer (mettre en œuvre et exécuter), Contrôler (surveiller et réexaminer) et Agir (maintenir et améliorer)] pour assurer la mise en œuvre, la maintenance et l'amélioration continue de l'efficacité du SMCA d'un organisme.

Cela assure un degré de cohérence avec d'autres normes de système de management, telles que l'ISO 9001, l'ISO 14001, l'ISO/IEC 20000-1, l'ISO/IEC 27001 et l'ISO 28000, permettant ainsi une mise en œuvre et un fonctionnement cohérents et intégrés avec les systèmes de management associés.

Conformément au cycle PDCA, les Articles 4 à 10 traitent des éléments suivants.

— L'Article 4 introduit les exigences nécessaires pour établir le contexte du SMCA applicable à l'organisme, ainsi que les besoins, les exigences et le domaine d'application.

— L'Article 5 résume les exigences spécifiques au rôle de la Direction générale dans le SMCA, et la manière dont le leadership communique ses attentes à l'organisme par le biais d'une déclaration de politique.

— L'Article 6 décrit les exigences pour établir des objectifs stratégiques et des principes d'orientation pour le SMCA dans sa globalité.

— L'Article 7 vient à l'appui des opérations du SMCA en lien avec la détermination des compétences et la communication avec les parties intéressées, sur une base récurrente ou en tant que de besoin, tout en documentant, maîtrisant, maintenant et conservant les informations documentées requises.

— L'Article 8 définit les besoins de continuité d'activité, détermine la manière de les traiter et développe les procédures afin de gérer l'organisme durant une perturbation.

— L'Article 9 résume les exigences nécessaires pour mesurer la performance de la continuité d'activité, la conformité du SMCA au présent document et le pilotage de la revue de direction.

— L'Article 10 identifie et intervient sur une non-conformité du SMCA et sur l'amélioration continue par le biais d'une action corrective.

0.4 Contenu du présent document

Le présent document se conforme aux exigences de l'ISO relatives aux normes de systèmes de management. Ces exigences comprennent une structure-cadre, un texte de base identique et des termes

communs avec des définitions clés, élaborés à l'attention des utilisateurs mettant en œuvre plusieurs normes ISO de systèmes de management.

Le présent document ne comporte pas d'exigences spécifiques à d'autres systèmes de management, bien que ses éléments puissent être alignés ou intégrés avec ceux d'autres systèmes de management.

Le présent document contient des exigences qui peuvent être utilisées par un organisme pour mettre en œuvre un SMCA et en apprécier la conformité. Un organisme souhaitant démontrer la conformité au présent document peut le faire:

— en réalisant une auto-évaluation et une auto-déclaration; ou

— en recherchant la confirmation de sa conformité par des parties ayant un intérêt dans l'organisme, telles que les clients; ou

— en recherchant la confirmation de son auto-déclaration par une partie externe à l'organisme; ou

— en recherchant la certification/l'enregistrement de son SMCA par un organisme externe.

Les Articles 1 à 3 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 contiennent les exigences à utiliser pour apprécier la conformité au présent document.

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

a) le verbe «devoir» indique une exigence;

b) l'expression «il convient de» indique une recommandation;

c) le verbe «pouvoir» (may) indique une permission;

d) le verbe «pouvoir» (can) indique une possibilité ou capacité.

Les informations sous forme de «NOTE» sont fournies pour faciliter la compréhension de l'exigence associée ou la clarifier. Les «Notes à l'article» employées à l'Article 3 fournissent des informations supplémentaires qui viennent compléter les données terminologiques et peuvent contenir des dispositions concernant l'usage d'un terme.

NORME INTERNATIONALE **ISO 22301:2019(F)**

Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences

1 Domaine d'application

Le présent document spécifie les exigences pour mettre en œuvre, maintenir et améliorer un système de management afin de se protéger contre les perturbations, réduire la vraisemblance de leur survenance, s'y préparer, y répondre et se rétablir lorsqu'elles se produisent.

Les exigences spécifiées dans le présent document sont génériques et prévues pour être applicables à tous les organismes, ou à des parties de ceux-ci, indépendamment du type, de la taille et de la nature de l'organisme. Le champ d'application de ces exigences dépend de l'environnement et de la complexité de fonctionnement de l'organisme.

Le présent document est applicable à tous les types et toutes les tailles d'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.

Le présent document peut être utilisé pour apprécier l'aptitude d'un organisme à satisfaire ses propres besoins et obligations en matière de continuité d'activité.

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/

NOTE Les termes et définitions ci-dessous remplacent ceux donnés dans l'ISO 22300:2018.

3.1
activité
ensemble d'une ou plusieurs tâches ayant une finalité définie

[SOURCE: ISO 22300:2018, 3.1, modifiée — La définition a été remplacée et l'exemple a été supprimé.]