NORME INTERNATIONALE

ISO 22301

Première édition
2012-05-15

Sécurité sociétale — Systèmes de management de la continuité d'activité — Exigences

Societal security — Business continuity management systems — Requirements

Numéro de référence
ISO 22301:2012(F)

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

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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

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.

L'ISO 22301 a été élaborée par le comité technique ISO/TC 223, *Sécurité sociétale*.

La présente version française de l'ISO 22301 correspond à la version anglaise publiée le 2012-05-15 et corrigée le 2012-06-15.

0 Introduction

0.1 Généralités

La présente Norme internationale spécifie les exigences relatives à l'établissement et au management d'un Système de Management de la Continuité d'Activité (SMCA) efficace.

Un SMCA souligne l'importance :

— d'une compréhension des besoins de l'organisation et de la nécessité de mettre en place une politique et des objectifs en matière de management de la continuité d'activité ;

— de la mise en œuvre et de l'exploitation de contrôles et de mesures de gestion de la capacité globale d'une organisation à gérer des incidents perturbateurs ;

— d'une surveillance et d'une revue des performances et de l'efficacité du SMCA ; et

— d'une amélioration continue sur la base de mesures objectives.

Comme tout autre système de management, un SMCA intègre les éléments clés suivants :

a) une politique ;

b) des personnes ayant des responsabilités définies ;

c) des processus de management se rapportant à :

   1) la politique ;

   2) la planification ;

   3) la mise en œuvre et le fonctionnement ;

   4) l'évaluation des performances ;

   5) la revue de direction ; et

   6) l'amélioration ;

d) une documentation fournissant des preuves tangibles ; et

e) tous les processus de management de la continuité d'activité pertinents pour l'organisation.

La continuité d'activité contribue à rendre la société plus résiliente. Il est possible qu'il faille impliquer dans le processus de reprise la communauté dans son ensemble, ainsi que l'impact de l'environnement de l'organisation et donc l'impact des autres organisations sur l'organisation elle-même.

0.2 Le modèle Planifier-Déployer-Contrôler-Agir (Plan-Do-Check-Act, PDCA)

La présente Norme internationale applique le modèle PDCA à la planification, l'établissement, la mise en œuvre, le fonctionnement, la surveillance, la revue, le maintien et l'amélioration continue de l'efficacité du SMCA d'une organisation.

Ceci assure un degré de cohérence avec d'autres normes de système de management, telles que l'ISO 9001, *Systèmes de management de la qualité*, l'ISO 14001, *Systèmes de management environnemental*, l'ISO/CEI 27001, *Systèmes de management de la sécurité de l'information*, l'ISO/CEI 20000-1, *Technologies de l'information — Gestion des services* et l'ISO 28000, *Spécifications relatives aux systèmes de management de la sûreté de la chaîne d'approvisionnement*, permettant ainsi une mise en œuvre et un fonctionnement cohérents et intégrés avec les systèmes de management associés.

La Figure 1 illustre comment un SMCA prend pour entrées les parties intéressées, les exigences de management de la continuité et comment, via les actions et les processus nécessaires, il produit des sorties en matière de continuité (c'est-à-dire une continuité de l'activité gérée) qui satisfont à ces exigences.

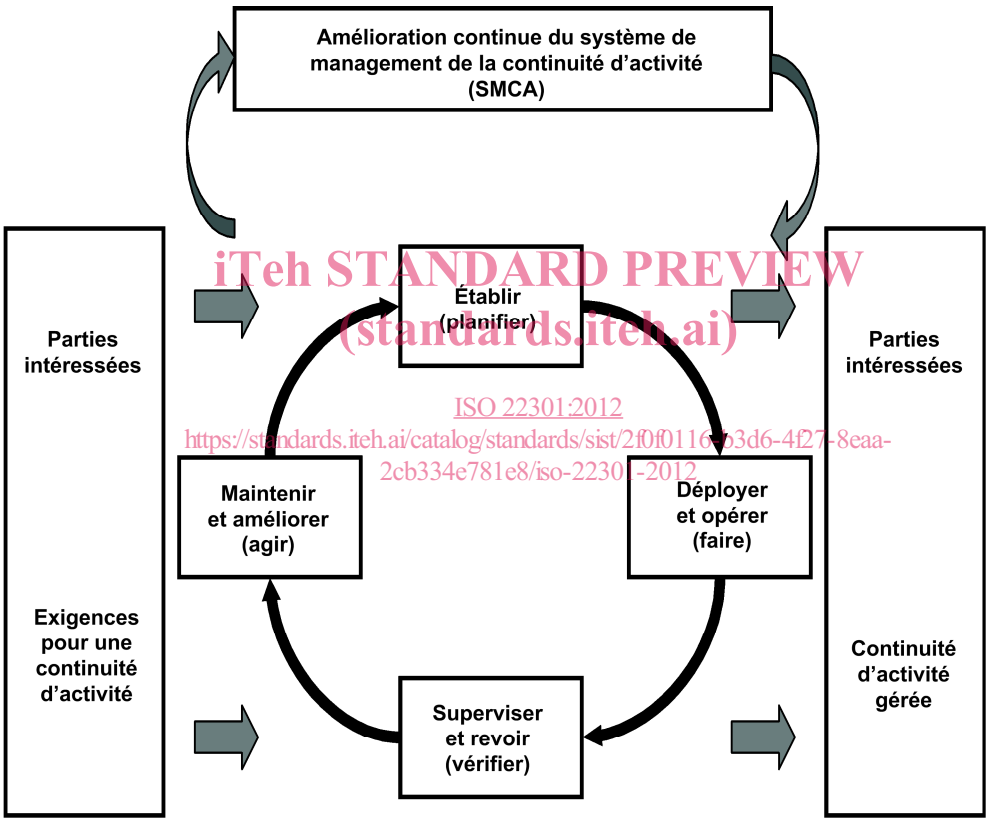

Figure 1 — Modèle PDCA appliqué aux processus d'un SMCA

Tableau 1 — Explication du modèle PDCA

Planifier (Établir)	Établir une politique, des objectifs, des cibles, des contrôles, des processus et des procédures de continuité d'activité pertinents pour améliorer la continuité d'activité afin d'obtenir des résultats alignés avec les politiques et les objectifs globaux de l'organisation.
Déployer (Mettre en place et en œuvre)	Mettre en œuvre et rendre opérationnels la politique, les contrôles, les processus et les procédures de continuité d'activité.
Contrôler (Superviser et réviser)	Superviser et revoir les performances par rapport à la politique et aux objectifs de continuité d'activité, rendre compte des résultats à la direction pour revue et déterminer et autoriser des actions correctives et d'amélioration.
Agir (Maintenir et améliorer)	Maintenir et améliorer le SMCA en entreprenant des actions correctives, sur la base des résultats de la revue de direction, et en reconsidérant le périmètre du SMCA ainsi que la politique et les objectifs de continuité d'activité.

0.3 Éléments du modèle PDCA dans la présente Norme internationale

Dans le modèle PDCA présenté dans le Tableau 1, les Articles 4 à 10 de la présente Norme internationale traitent des éléments suivants :

— l'Article 4 est une partie du thème « Planifier ». Il introduit les exigences nécessaires pour établir le contexte du SMCA tel qu'il s'applique à l'organisation, ainsi que les besoins, les exigences et le périmètre.

— l'Article 5 est une partie du thème « Planifier ». Il résume les exigences spécifiques au rôle joué par la Direction dans le SMCA, et la manière dont la Direction communique ses attentes à l'organisation par le biais d'une déclaration de politique.

— l'Article 6 est une partie du thème « Planifier ». Il décrit les exigences relatives à l'établissement des objectifs stratégiques et des principes directeurs du SMCA dans son ensemble. Le contenu de l'Article 6 ne consiste pas à mettre en place les solutions de traitement des risques découlant de l'appréciation des risques, ni à établir les objectifs de reprise issus de l'analyse d'impact sur l'activité.

NOTE Les exigences relatives à l'analyse d'impact sur l'activité et au processus d'appréciation du risque sont spécifiées de manière détaillée à l'Article 8.

— l'Article 7 est une partie du thème « Planifier ». Il vient à l'appui des opérations du SMCA relatives à la détermination des compétences et à l'établissement de communications avec les parties intéressées, sur une base récurrente/au besoin, tout en documentant, contrôlant, tenant à jour et conservant la documentation requise.

— l'Article 8 est une partie du thème « Faire ». Il définit les exigences relatives à la continuité d'activité, détermine la manière de les traiter et développe les procédures afin de gérer un incident perturbateur.

— l'Article 9 est une partie du thème « Contrôler ». Il résume les exigences nécessaires pour mesurer la performance du management de la continuité d'activité, la conformité du SMCA à la présente Norme internationale et aux attentes de la Direction, et recherche les retours d'information de la direction concernant les attentes.

— l'Article 10 est une partie du thème « Agir ». Il identifie et intervient sur une non-conformité du SMCA par le biais d'une action corrective.

Sécurité sociétale — Systèmes de management de la continuité d'activité — Exigences

1 Domaine d'application

La présente Norme internationale relative à la gestion de la continuité d'activité spécifie les exigences pour planifier, établir, mettre en place et en œuvre, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent.

Les exigences spécifiées dans la présente Norme internationale sont génériques et prévues pour être applicables à toutes les organisations, ou parties de celles-ci, indépendamment du type, de la taille et de la nature de l'organisation. Le champ d'application de ces exigences dépend de l'environnement et de la complexité de fonctionnement de l'organisation.

La présente Norme internationale ne vise pas à uniformiser la structure d'un système de management de la continuité d'activité (SMCA), mais à permettre à une organisation de concevoir un SMCA qui soit adapté à ses besoins et qui satisfasse aux exigences des parties intéressées. Ces besoins sont façonnés par les exigences juridiques, réglementaires, organisationnelles et industrielles, les produits et les services, les processus employés, la taille et la structure de l'organisation et les exigences des parties intéressées.

La présente Norme internationale est applicable à tous les types et toutes les tailles d'organisations souhaitant :

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

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

c) démontrer cette conformité à des tiers ;

d) faire certifier/enregistrer son SMCA par un organisme de certification tiers et accrédité ; ou

e) réaliser une autoévaluation et une auto-déclaration de conformité à la présente Norme internationale.

La présente Norme internationale peut être utilisée pour évaluer la capacité d'une organisation à satisfaire ses propres besoins et obligations en matière de continuité.

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).

Il n'y a aucune référence normative.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
activité
processus ou ensemble de processus exécutés par une organisation (ou pour son compte) qui réalise ou aide à réaliser un ou plusieurs produits et services

EXEMPLE De tels processus comprennent la comptabilité, les centres d'appel, les technologies de l'information (IT), la fabrication, la distribution.

3.2
audit
processus systématique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

NOTE 1 Un audit peut être interne (de première partie) ou externe (de seconde ou tierce partie), et il peut être combiné (s'il associe deux disciplines ou plus).

NOTE 2 Les termes « preuves d'audit » et « critères d'audit » sont définis dans l'ISO 19011.

3.3
continuité d'activité
capacité de l'organisation à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur

[SOURCE : ISO 22300]

3.4
gestion de la continuité d'activité
processus de management holistique qui identifie les menaces potentielles pour une organisation ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeur

3.5
système de management de la continuité d'activité
SMCA
partie du système de management global qui établit, met en œuvre, opère, contrôle, révise, maintient et améliore la continuité d'activité

NOTE Le système de management comprend la structure organisationnelle, les politiques, les planifications, les responsabilités, les procédures, les processus et les ressources.

3.6
plan de continuité d'activité
procédures documentées servant de guide aux organisations pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation

NOTE Ce plan couvre généralement les ressources, les services et les activités requis pour assurer la continuité des fonctions critiques.

3.7
programme de continuité d'activité
processus continu de management et de gouvernance soutenu par la direction et doté de ressources appropriées pour mettre en œuvre et maintenir le management de la continuité d'activité

3.8
analyse d'impact sur l'activité
processus d'analyse des activités et de l'effet qu'une perturbation de l'activité peut avoir sur elles

[SOURCE : ISO 22300]

3.9
compétence
aptitude à mettre en pratique des connaissances et un savoir-faire pour obtenir les résultats escomptés

3.10
conformité
satisfaction d'une exigence

[SOURCE : ISO 22300]

3.11
amélioration continue
activité récurrente visant à améliorer les performances

[SOURCE : ISO 22300]

3.12
correction
action visant à éliminer une non-conformité détectée

[SOURCE : ISO 22300]

3.13
action corrective
action visant à éliminer la cause d'une non-conformité et à éviter sa réapparition

NOTE Dans le cas d'autres résultats indésirables, il est nécessaire d'entreprendre une action visant à réduire au minimum ou éliminer les causes et à réduire leur impact ou éviter leur réapparition. De telles actions ne relèvent pas du concept « d'action corrective » au sens de la présente définition.

[SOURCE : ISO 22300]

3.14
document
support d'information et l'information qu'il contient

NOTE 1 Le support peut être du papier, un disque informatique magnétique, électronique ou optique, une photographie ou une configuration de référence, ou une combinaison de ceux-ci.

NOTE 2 Un ensemble de documents, par exemple des spécifications et des enregistrements, est souvent appelé « documentation ».

3.15
information documentée
information qui nécessite d'être contrôlée et tenue à jour par une organisation et support sur lequel elle est contenue

NOTE 1 Les informations documentées peuvent se présenter dans tout format et sur tout support et provenir de toute source.

NOTE 2 Les informations documentées peuvent se référer :

— au système de management, y compris les processus associés ;

— aux informations générées en vue du fonctionnement de l'organisation (documentation) ;

— aux preuves des résultats obtenus (enregistrements).

3.16
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

[SOURCE : ISO 22300]

3.17
événement
occurrence ou changement d'un ensemble particulier de circonstances

NOTE 1 Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.

NOTE 2 Un événement peut consister en quelque chose qui ne se produit pas.

NOTE 3 Un événement peut parfois être qualifié « d'incident » ou « d'accident ».

NOTE 4 Un événement sans conséquences peut également être appelé « quasi-accident » ou « incident » ou « presque succès ».

[SOURCE : ISO/CEI Guide 73]

3.18
exercice

processus visant à se former, évaluer, mettre en pratique et améliorer les performances au sein d'une organisation

NOTE 1 Des exercices peuvent être utilisés pour : valider des politiques, des plans, des procédures, une formation, un équipement et des accords entre organisations ; clarifier et former le personnel à des rôles et des responsabilités ; améliorer la coordination et les communications entre organisations ; identifier les lacunes en matière de ressources ; améliorer les performances individuelles et identifier les opportunités d'amélioration et les opportunités contrôlées d'improvisation.

NOTE 2 Un test est un type unique et particulier d'exercice qui intègre l'attente de la réussite ou de l'échec d'un élément parmi les buts ou les objectifs de l'exercice planifié.

[SOURCE : ISO 22300]

3.19
incident
situation qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise

[SOURCE : ISO 22300]

3.20
infrastructure
système d'installations, d'équipements et de services nécessaire au fonctionnement d'une organisation

