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

*Security and resilience — Business continuity management systems
— Requirements*

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO 22301:2019](https://standards.itih.ai/catalog/standards/iso/914fc1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019)

<https://standards.itih.ai/catalog/standards/iso/914fc1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO 22301:2019](https://standards.iteh.ai/catalog/standards/iso/914fc1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019)

<https://standards.iteh.ai/catalog/standards/iso/914fc1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2019

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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	v
Introduction	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Contexte de l'organisme	7
4.1 Compréhension de l'organisme et de son contexte.....	7
4.2 Compréhension des besoins et attentes des parties intéressées.....	7
4.2.1 Généralités.....	7
4.2.2 Exigences réglementaires et juridiques.....	8
4.3 Détermination du domaine d'application du système de management de la continuité d'activité.....	8
4.3.1 Généralités.....	8
4.3.2 Domaine d'application du système de management de la continuité d'activité.....	8
4.4 Système de management de la continuité d'activité.....	8
5 Leadership	8
5.1 Leadership et engagement.....	8
5.2 Politique.....	9
5.2.1 Établissement de la politique de continuité d'activité.....	9
5.2.2 Communication de la politique de continuité d'activité.....	9
5.3 Rôles, responsabilités et autorités.....	9
6 Planification	10
6.1 Actions face aux risques et opportunités.....	10
6.1.1 Détermination des risques et opportunités.....	10
6.1.2 Gestion des risques et opportunités.....	10
6.2 Objectifs de continuité d'activité et planification pour les atteindre.....	10
6.2.1 Établissement des objectifs de continuité d'activité.....	10
6.2.2 Détermination des objectifs de continuité d'activité.....	10
6.3 Planification des modifications du système de management de la continuité d'activité.....	11
7 Support	11
7.1 Ressources.....	11
7.2 Compétences.....	11
7.3 Sensibilisation (prise de conscience).....	11
7.4 Communication.....	12
7.5 Informations documentées.....	12
7.5.1 Généralités.....	12
7.5.2 Création et mise à jour.....	12
7.5.3 Maîtrise des informations documentées.....	12
8 Fonctionnement	13
8.1 Planification opérationnelle et maîtrise.....	13
8.2 Bilan d'impact sur l'activité et appréciation du risque.....	13
8.2.1 Généralités.....	13
8.2.2 Bilan d'impact sur l'activité.....	13
8.2.3 Appréciation du risque.....	14
8.3 Stratégies et solutions de continuité d'activité.....	14
8.3.1 Généralités.....	14
8.3.2 Identification des stratégies et solutions.....	14
8.3.3 Sélection des stratégies et solutions.....	15
8.3.4 Exigences de ressources.....	15
8.3.5 Mise en œuvre des solutions.....	15
8.4 Plans et procédures de continuité d'activité.....	15

8.4.1	Généralités	15
8.4.2	Structure de réponse	16
8.4.3	Avertissement et communication	16
8.4.4	Plans de continuité d'activité	17
8.4.5	Rétablissement	18
8.5	Programme d'exercices	18
8.6	Évaluation de la documentation et des capacités de continuité d'activité	18
9	Évaluation de la performance	19
9.1	Surveillance, mesurage, analyse et évaluation	19
9.2	Audit interne	19
9.2.1	Généralités	19
9.2.2	Programme(s) d'audit	19
9.3	Revue de direction	20
9.3.1	Généralités	20
9.3.2	Éléments d'entrée de la revue de direction	20
9.3.3	Éléments de sortie de la revue de direction	20
10	Amélioration	21
10.1	Non-conformité et actions correctives	21
10.2	Amélioration continue	21
	Bibliographie	22

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO 22301:2019](https://standards.iteh.ai/catalog/standards/iso/914fc1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019)

<https://standards.iteh.ai/catalog/standards/iso/914fc1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019>

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.

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

[ISO 22301:2019](#)

<https://standards.iteh.ai/catalog/standards/iso/914fe1f6-d57c-4e0b-b9d5-3704af15aa58/iso-22301-2019>

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.]

3.2 audit

processus (3.26) méthodique, indépendant et documenté en vue 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 à l'article: Un audit peut être interne (audit de première partie), externe (audit de seconde ou de tierce partie) ou combiné (combinant deux disciplines ou plus).

Note 2 à l'article: Un audit interne est réalisé par l'organisme (3.21) lui-même ou par une partie externe pour le compte de celui-ci.

Note 3 à l'article: Les termes «preuves d'audit» et «critères d'audit» sont définis dans l'ISO 19011.

Note 4 à l'article: Les éléments fondamentaux d'un audit comprennent la détermination de la *conformité* (3.7) d'un objet selon une procédure réalisée par du personnel n'étant pas responsable de l'objet audité.

Note 5 à l'article: Un audit interne peut être réalisé pour une revue de direction et d'autres besoins internes et peut servir de base à la déclaration de conformité de l'organisme. L'indépendance peut être démontrée par l'absence de responsabilité vis-à-vis de l'activité (3.1) à auditer. Les audits externes comprennent les audits de seconde et de tierce partie. Les audits de seconde partie sont réalisés par des parties ayant un intérêt à l'égard de l'organisme, comme les clients, ou d'autres personnes agissant en leur nom. Les audits de tierce partie sont réalisés par des organismes d'audit externes et indépendants tels que ceux qui octroient la certification/l'enregistrement de conformité ou des organismes publics.

Note 6 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO. La définition initiale a été modifiée par l'ajout des Notes 4 et 5 à l'article.

3.3 continuité d'activité

capacité d'un organisme (3.21) à poursuivre la livraison de *produits* et la fourniture de *services* (3.27) dans des délais acceptables à une capacité prédéfinie durant une *perturbation* (3.10)

[SOURCE: ISO 22300:2018, 3.24, modifiée — La définition a été remplacée.]

3.4 plan de continuité d'activité

informations documentées (3.11) servant de guide à un organisme (3.21) pour répondre à une *perturbation* (3.10) et reprendre, rétablir et restaurer la livraison de *produits* et la fourniture de *services* (3.27) en cohérence avec ses *objectifs* (3.20) de *continuité d'activité* (3.3)

[SOURCE: ISO 22300:2018, 3.27, modifiée — La définition a été remplacée et la Note 1 à l'article a été supprimée.]

3.5 bilan d'impact sur l'activité

processus (3.26) d'analyse de l'impact (3.13) dans le temps d'une *perturbation* (3.10) sur l'organisme (3.21)

Note 1 à l'article: Le résultat est un inventaire des *exigences* (3.28) de *continuité d'activité* (3.3) et leur justification.

[SOURCE: ISO 22300:2018, 3.29, modifiée — La définition a été remplacée et la Note 1 à l'article a été ajoutée.]

3.6 compétence

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

Note 1 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO.

3.7**conformité**

satisfaction d'une *exigence* (3.28)

Note 1 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO.

3.8**amélioration continue**

activité (3.1) récurrente permettant d'améliorer les *performances* (3.23)

Note 1 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO.

3.9**action corrective**

action visant à éliminer la ou les cause(s) d'une *non-conformité* (3.19) et à éviter sa réapparition

Note 1 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO.

3.10**perturbation**

incident (3.14), anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la livraison de *produits* et à la fourniture de *services* (3.27) prévues selon les *objectifs* (3.20) d'un *organisme* (3.21)

[SOURCE: ISO 22300:2018, 3.70, modifiée — La définition a été remplacée.]

3.11**information documentée**

information devant être maîtrisée et tenue à jour par un *organisme* (3.21) ainsi que le support sur lequel elle figure

Note 1 à l'article: Les informations documentées peuvent se présenter sous n'importe quel format et sur tous supports et peuvent provenir de toute source.

Note 2 à l'article: Les informations documentées peuvent se rapporter:

- au *système de management* (3.16), y compris aux *processus* (3.26) connexes;
- aux informations créées en vue du fonctionnement de l'organisme (documentation);
- aux preuves des résultats obtenus (enregistrements).

Note 3 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO.

3.12**efficacité**

niveau de réalisation des *activités* (3.1) planifiées et d'obtention des résultats escomptés

Note 1 à l'article: Cela constitue l'un des termes communs et l'une des définitions essentielles de la structure-cadre (HLS) des normes de système de management ISO.

3.13**impact**

résultat d'une *perturbation* (3.10) affectant les *objectifs* (3.20)

[SOURCE: ISO 22300:2018, 3.107, modifiée — La définition a été remplacée.]