PROJET DE NORME INTERNATIONALE

ISO/DIS 22301

ISO/TC **292**	Secrétariat: **SIS**
Début de vote: **2019-01-03**	Vote clos le: **2019-03-28**

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

Security and resilience — Business continuity management systems — Requirements

ICS: 03.100.01; 03.100.70

TRAITEMENT PARALLÈLE ISO/CEN

Numéro de référence
ISO/DIS 22301:2019(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Website: 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 le lien suivant : www.iso.org/iso/fr/avant-propos.html.

L'ISO 22301 a été élaborée par le comité technique ISO/TC 292, *Sécurité et résilience*.

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) efficace.

Il convient qu'un organisme développe une continuité d'activité appropriée à l'importance et au type d'impact qu'il 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 fournis, 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 les performances 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 :

la politique ;

la planification ;

la mise en œuvre et le fonctionnement ;

l'appréciation des performances ;

la revue de direction ;

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 SMCA

Le 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 :

— contribue à ses objectifs stratégiques ;

— acquiert un avantage concurrentiel ;

— protège et renforce sa réputation et sa crédibilité ;

— contribue à la résilience de l'organisme ;

b) d'un point de vue financier :

— rend les partenaires commerciaux confiants en sa réussite ;

— réduit l'exposition juridique et financière ;

— diminue les coûts directs et indirects des perturbations ;

c) du point de vue des parties intéressées :

— protège la vie, la propriété et l'environnement ;

— prend en considération les attentes des parties intéressées ;

d) du point de vue des processus internes :

— améliore sa capacité à rester efficace pendant les perturbations ;

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

— traite les vulnérabilités opérationnelles.

0.3 Le modèle Planifier-Faire-Vérifier-Agir (Plan-Do-Check-Act, PDCA)

Le présent document applique le modèle 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.

Cela 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/IEC 27001, *Systèmes de management de la sécurité de l'information*, l'ISO/IEC 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.

0.4 Éléments du modèle PDCA dans le présent document

Dans le modèle PDCA, les Articles 4 à 10 du présent document traitent des éléments suivants.

L'Article 4 est une composante du volet « Planifier ». Il introduit les exigences nécessaires pour établir le contexte du SMCA tel qu'il s'applique à l'organisme, ainsi que les besoins, les exigences et le domaine d'application.

L'Article 5 est une composante du volet « Planifier ». Il résume les exigences spécifiques au rôle de la Direction 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 est une composante du volet « Planifier ». Il décrit les exigences relatives à l'établissement des objectifs stratégiques et des principes directeurs du SMCA dans son ensemble.

L'Article 7 est une composante du volet « Planifier ». Il vient à l'appui des opérations du SMCA dans la mesure où elles portent sur 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 est une composante du volet « Faire ». Il définit les besoins de continuité d'activité, détermine la manière de les traiter et développe les procédures afin de gérer l'organisme pendant une perturbation.

L'Article 9 est une composante du volet « Vérifier ». Il résume les exigences nécessaires pour mesurer la performance de la continuité d'activité, la conformité du SMCA au présent document et à la revue de direction.

L'Article 10 est une composante du volet « Agir ». Il identifie et intervient sur une non-conformité du SMCA et sur l'amélioration continue par le biais d'une action corrective.

0.5 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 avec ou intégrés à ces 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 autoévaluation 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 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, tandis que 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 une 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 planifier, établir, mettre en œuvre, faire fonctionner, surveiller, passer en revue, maintenir et améliorer de manière continue 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 apparaissent.

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 délivrance de produits et de services à un niveau de capacité acceptable et préalablement défini lors d'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

Le présent document ne contient aucune référence normative.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions 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 http://www.iso.org/obp

— IEC Electropedia : disponible à l'adresse http://www.electropedia.org

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

[SOURCE : ISO 22300:2018, 3.1, modifiée. Note à l'article supprimée.]

3.2
audit
processus (3.40) 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 : Les éléments fondamentaux d'un audit comprennent la détermination de la *conformité* (3.8) d'un *objet* (3.29) selon une *procédure* (3.39) réalisée par du *personnel* (3.35) n'étant pas responsable de l'objet audité.

Note 2 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 3 à l'article : Un audit interne est réalisé par l'organisme ou par une partie externe pour son compte. Un audit interne peut être réalisé pour une *revue* (3.47) 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.

Note 4 à l'article : Les audits externes comprennent les audits appelés généralement 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 5 à l'article : Les termes « preuves d'audit » et « critères d'audit » sont définis dans l'ISO 19011.

[SOURCE : ISO 22300:2018, 3.13, modifiée. Notes 5, 6 et 8 à l'article supprimées.]

3.3
continuité d'activité
capacité d'un *organisme* (3.31) à poursuivre la délivrance de produits et de services (3.41) dans des délais et à un niveau de capacité prédéfini acceptables relativement à une *perturbation* (3.12)

[SOURCE : ISO 22300:2018, 3.24, modifiée.]

3.4
système de management de la continuité d'activité
SMCA
système de management (3.25) destiné à la *continuité d'activité* (3.3)

Note 1 à l'article : Le système de management comprend la structure de l'organisme, les politiques, les *activités* (3.1) de *planification* (3.36), les responsabilités, les *procédures* (3.39), les *processus* (3.40) et les ressources.

[SOURCE : ISO 22300:2018, 3.26, modifiée.]

3.5
plan de continuité d'activité
informations documentées (3.13) servant de guide à un *organisme* (3.31) pour répondre à une *perturbation* (3.12) et reprendre, rétablir et restaurer la délivrance de produits et de services en cohérence avec ses objectifs de continuité d'activité

[SOURCE : ISO 22300:2018, 3.27, modifiée. Note 1 à l'article supprimée.]

3.6
bilan d'impact sur l'activité
processus (3.40) d'analyse de l'*impact* (3.18) d'une *perturbation* (3.12) sur l'*organisme* (3.31)

Note 1 à l'article : Le résultat est un état des *exigences* (3.45) de *continuité d'activité* (3.3) et leur justification.

[SOURCE : ISO 22300:2018, 3.29, modifiée. Note 1 à l'article ajoutée.]

3.7
compétence
aptitude à mettre en pratique des connaissances et des savoir-faire pour obtenir les résultats escomptés

[SOURCE : ISO 22300:2018, 3.44]

3.8
conformité
satisfaction d'une *exigence* (3.45)

[SOURCE : ISO 22300:2018, 3.45]

3.9
conséquence
répercussion d'un *événement* (3.16) affectant les *objectifs* (3.30)

Note 1 à l'article : Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs, directs ou indirects, sur les objectifs.

Note 2 à l'article : Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 3 à l'article : Toute conséquence peut s'accentuer par des réactions en chaîne.

[SOURCE : ISO 31000:2018, 3.6, modifiée.]

3.10
amélioration continue
activité (3.1) récurrente permettant d'améliorer les *performances* (3.33)

[SOURCE : ISO 22300:2018, 3.48]

3.11
action corrective
action visant à éliminer la cause d'une *non-conformité* (3.28) et à éviter sa réapparition

Note 1 à l'article : 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* (3.18) ou éviter leur réapparition. De telles actions ne relèvent pas du concept « d'action corrective » au sens de la présente définition.

[SOURCE : ISO 22300:2018, 3.54]

3.12
perturbation
incident (3.19), anticipé ou non anticipé, qui entraîne un écart négatif non planifié par rapport à la délivrance prévue de *produits ou services* (3.41) selon les *objectifs* (3.30) d'un *organisme* (3.31)

[SOURCE : ISO 22300:2018, 3.70, modifiée.]

3.13
information documentée
information (3.20) devant être maîtrisée et tenue à jour par un *organisme* (3.31) 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* (3.25), y compris les *processus* (3.40) connexes ;

aux informations créées en vue du fonctionnement de l'organisme (documentation) ;

aux preuves des résultats obtenus [*enregistrements* (3.43)].

[SOURCE : ISO 22300:2018, 3.72]

3.14
efficacité
niveau de réalisation des *activités* (3.1) planifiées et d'obtention des résultats escomptés

[SOURCE : ISO 22300:2018, 3.76]

3.15
urgence
occurrence ou *événement* (3.16) soudain, de cas d'urgence, généralement imprévu, qui nécessite une action rapide

Note 1 à l'article : Une urgence est généralement une *perturbation* (3.12) ou un état pouvant souvent être anticipé(e) ou planifié(e), mais rarement prévu avec exactitude.

[SOURCE : ISO 22300:2018, 3.77]

3.16
événement
occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article : Un événement peut être unique ou se reproduire et peut avoir plusieurs causes et plusieurs *conséquences* (3.9).

Note 2 à l'article : Un événement peut être quelque chose qui est attendu, mais qui ne se produit pas, ou quelque chose auquel on ne s'attend pas, mais qui se produit.

Note 3 à l'article : Un événement peut être une source de risque.

[SOURCE : ISO 31000:2018, 3.5]

3.17
exercice
processus (3.40) visant à se former, apprécier, mettre en pratique et améliorer les *performances* (3.33) au sein d'un *organisme* (3.31)

Note 1 à l'article : Des exercices peuvent être utilisés pour: valider des politiques, des plans, des *procédures* (3.39), une *formation* (3.54), un équipement et des accords entre organismes ; clarifier et former le *personnel* (3.35) à des rôles et des responsabilités ; améliorer la coordination et les communications entre organismes ; identifier les écarts en matière de ressources ; améliorer les performances individuelles et identifier les opportunités d'amélioration et fournir une opportunité maîtrisée de pratiquer l'improvisation. Un exercice n'a pas besoin de rechercher la réussite ou l'échec.

Note 2 à l'article : Voir également *test* (3.52).

[SOURCE : ISO 22300:2018, 3.83, modifiée.]

3.18
impact
résultat d'une *perturbation* (3.12) affectant les *objectifs* (3.30)

[SOURCE : ISO 22300:2018, 3.107, modifiée.]

3.19
incident
événement (3.16) qui peut être, ou conduire à, une *perturbation* (3.12), une perte, une *urgence* (3.15) ou une crise

[SOURCE : ISO 22300:2018, 3.111, modifiée.]

3.20
informations
données traitées, organisées et corrélées de manière à produire un sens

[SOURCE : ISO 22300:2018, 3.116]

3.21
partie intéressée
partie prenante
personne ou *organisme* (3.31) qui peut affecter, être affecté ou se percevoir comme affecté par une décision ou une *activité* (3.1)

EXEMPLE Clients, propriétaires, *personnel* (3.35), prestataires, établissements financiers, autorités réglementaires, syndicats, partenaires ou société pouvant inclure des concurrents ou des groupes de pression d'opposition.

Note 1 à l'article : Un décideur peut être une partie intéressée.

Note 2 à l'article : Les communautés impactées et les populations locales sont considérées comme des parties intéressées externes.

[SOURCE : ISO 22300:2018, 3.124, modifiée. L'exemple a été modifié. La Note 3 à l'article a été supprimée.]

3.22
audit interne
audit (3.2) réalisé par, ou pour le compte de, l'*organisme* (3.31) lui-même pour la *revue* (3.47) de direction et d'autres besoins internes et qui peut servir de base à l'autodéclaration de *conformité* (3.8) de l'organisme

Note 1 à l'article : Dans de nombreux cas, et en particulier pour les petits organismes, l'indépendance peut être démontrée par l'absence de responsabilité vis-à-vis de l'*activité* (3.1) à auditer.

[SOURCE : ISO 22300:2018, 3.126]

3.23
vraisemblance
possibilité que quelque chose se produise

Note 1 à l'article : Dans la terminologie du *management du risque* (3.50), le mot « vraisemblance » est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article : Le terme anglais « likelihood » (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme « probability » (probabilité) qui est utilisé à la place. En anglais, cependant, le terme « probability » (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme « vraisemblance » est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme « probability » (probabilité) dans de nombreuses langues autres que l'anglais.

[SOURCE : ISO 31000:2018, 3.7]

3.24
management
activités (3.1) coordonnées pour diriger et contrôler un *organisme* (3.31)

[SOURCE : ISO 22300:2018, 3.135]

3.25
système de management
ensemble d'éléments corrélés ou en interaction d'un *organisme* (3.31), utilisés pour établir des *politiques* (3.37), des *objectifs* (3.30), et des *processus* (3.40) de façon à atteindre ces objectifs

Note 1 à l'article : Un système de management peut traiter d'une seule ou de plusieurs disciplines.

Note 2 à l'article : Les éléments du système comprennent la structure, les rôles et responsabilités, la *planification* (3.36) et le fonctionnement de l'organisme.

Note 3 à l'article : Le domaine d'application d'un système de management peut comprendre l'ensemble de l'organisme, des fonctions spécifiques et identifiées de l'organisme, des sections spécifiques et identifiées de l'organisme, ou une ou plusieurs fonctions à travers un groupe d'organismes.

[SOURCE : ISO 22300:2018, 3.137, modifiée.]

3.26
mesurage
processus (3.40) visant à déterminer une valeur

[SOURCE : ISO 22300:2018, 3.143, modifiée.]

3.27
surveillance
détermination de l'état d'un système, d'un *processus* (3.40) ou d'une *activité* (3.1)

[SOURCE : ISO 22300:2018, 3.147, modifiée.]

3.28
non-conformité
non-satisfaction d'une *exigence* (3.45)

[SOURCE : ISO 22300:2018, 3.149]

3.29
objet
entité unique et distincte pouvant être identifiée

[SOURCE : ISO 22300:2018, 3.151]

3.30
objectif
résultat à atteindre

Note 1 à l'article : Un objectif peut être stratégique, tactique ou opérationnel.

Note 2 à l'article : Les objectifs peuvent se rapporter à différentes disciplines (telles que finance, santé et sécurité et environnement) et peuvent s'appliquer à divers niveaux [par exemple au niveau stratégique, à un niveau concernant l'organisme dans son ensemble ou afférant à un projet, un produit ou un *processus* (3.40)].

Note 3 à l'article : Un objectif peut être exprimé de différentes manières, par exemple par un résultat escompté, un besoin, un critère opérationnel ou par l'utilisation d'autres termes ayant la même signification (par exemple finalité, but ou cible).

Note 4 à l'article : Dans le contexte des *systèmes de management de la continuité d'activité* (3.4), les objectifs de continuité d'activité sont fixés par l'organisme, en cohérence avec sa *politique* (3.37) de continuité d'activité, en vue d'atteindre des résultats spécifiques.

[SOURCE : ISO 22300:2018, 3.153. La Note 4 à l'article a été modifiée pour s'adapter au SMCA.]

3.31
organisme
personne ou groupe de personnes ayant ses propres fonctions, avec des responsabilités, des autorités et des relations lui permettant d'atteindre ses *objectifs* (3.30)

Note 1 à l'article : Le concept d'organisme englobe, sans s'y limiter, les travailleurs indépendants, les compagnies, les sociétés, les firmes, les entreprises, les administrations, les partenariats, les organisations caritatives ou les institutions, ou bien une partie ou une combinaison des entités précédentes, à responsabilité limitée ou ayant un autre statut, de droit public ou privé.

Note 2 à l'article : Pour les organismes ayant plusieurs unités d'exploitation, une seule unité d'exploitation peut être définie en tant qu'organisme.

[SOURCE : ISO 22300:2018, 3.158, modifiée.]

3.32
externaliser
passer un accord selon lequel un *organisme* (3.31) externe assure une partie de la fonction ou met en œuvre une partie du *processus* (3.40) d'un organisme

Note 1 à l'article : L'organisme externe n'est pas inclus dans le périmètre du *système de management* (3.25), contrairement à la fonction ou au processus externalisé qui en font partie intégrante.

[SOURCE : ISO 22300:2018, 3.160]

3.33
performance
résultat mesurable

Note 1 à l'article : Les performances peuvent être liées à des constats quantitatifs ou qualitatifs.

Note 2 à l'article : Les performances peuvent concerner le *management* (3.24) d'*activités* (3.1), de *processus* (3.40), de produits et services, de systèmes ou d'*organismes* (3.31).

[SOURCE : ISO 22300:2018, 3.167, modifiée. Mention de « produits et services ».]

3.34
évaluation de la performance
processus (3.40) visant à déterminer des résultats mesurables par rapport aux critères définis

[SOURCE : ISO 22300:2018, 3.168, modifiée. Ajout de « par rapport aux critères définis ».]

3.35
personnel
personnes travaillant pour un *organisme* (3.31) et sous le contrôle de celui-ci

Note 1 à l'article : Le concept de personnel inclut, sans toutefois s'y limiter, les employés, le personnel à temps partiel et le personnel intérimaire.

[SOURCE : ISO 22300:2018, 3.169]

3.36
planification
partie du *management* (3.24) consacrée à définir les *objectifs* (3.30) de *continuité d'activité* (3.3) et à spécifier les *processus* (3.30) opérationnels nécessaires et les ressources associées afin de remplir les objectifs de continuité d'activité

[SOURCE : ISO 22300:2018, 3.170, modifiée pour s'adapter à la « continuité d'activité ».]

3.37
politique
intentions et orientations d'un *organisme* (3.31), telles qu'elles sont officiellement formulées par sa *direction* (3.53)

[SOURCE : ISO 22300:2018, 3.171, modifiée pour inclure une virgule.]

3.38
activité prioritaire
activité (3.1) pour laquelle l'urgence est reconnue afin d'éviter des impacts inacceptables sur l'activité pendant une *perturbation* (3.12)

[SOURCE : ISO 22300:2018, 3.176, modifiée.]

3.39
procédure
manière spécifiée d'effectuer une *activité* (3.1) ou un *processus* (3.40)

Note 1 à l'article : Les procédures peuvent ou non faire l'objet de documents.

Note 2 à l'article : Lorsqu'une procédure fait l'objet de documents, les termes « procédure écrite » ou « procédure documentée » sont fréquemment utilisés. Le document contenant une procédure peut être appelé un « document de procédure ».

[SOURCE : ISO 22300:2018, 3.179]

3.40
processus
ensemble d'*activités* (3.1) corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

[SOURCE : ISO 22300:2018, 3.180, modifiée.]

3.41
produit ou service
élément de sortie ou résultat fourni par un *organisme* (3.31) à des *parties intéressées* (3.21)

EXEMPLE Articles manufacturés, assurance automobile et soins infirmiers communautaires.

[SOURCE : ISO 22300:2018, 3.181, modifiée.]

3.42
protection
mesures protégeant un *organisme* (3.31) et lui permettant de prévenir ou de limiter l'*impact* (3.18) d'une *perturbation* (3.12) potentielle

[SOURCE : ISO 22300:2018, 3.182 modifiée.]

3.43
enregistrement
document faisant état de résultats obtenus ou apportant la preuve de la réalisation d'une *activité* (3.1)

[SOURCE : ISO 22300:2018, 3.186]

3.44
rétablissement
restauration et amélioration, le cas échéant, des opérations, des installations, des moyens de subsistance ou des conditions de vie des *organismes* (3.31) affectés, y compris les efforts pour réduire les facteurs de *risque* (3.48)

[SOURCE : ISO 22300:2018, 3.187]

3.45
exigence
besoin ou attente formulé, généralement implicite ou obligatoire

Note 1 à l'article : « Généralement implicite » signifie qu'il est habituel ou courant, pour l'*organisme* (3.31) et les *parties intéressées* (3.21), que le besoin ou l'attente en question soit implicite.

Note 2 à l'article : Une exigence spécifiée est une exigence formulée, par exemple une *information documentée* (3.13).

[SOURCE : ISO 22300:2018, 3.190]

3.46
résilience
capacité d'assimilation et d'adaptation dans un environnement changeant

[SOURCE : ISO 22300:2018, 3.192]

3.47
revue
activité (3.1) entreprise afin de déterminer l'adaptation, l'adéquation et l'*efficacité* (3.14) du *système de management* (3.25) et de ses composantes pour atteindre les *objectifs* (3.30) établis

[SOURCE : ISO 22300:2018, 3.197]

3.48
risque
effet de l'incertitude sur les *objectifs* (3.30)

Note 1 à l'article : Un effet est un écart par rapport à une attente. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou résulter en des opportunités et des menaces.

Note 2 à l'article : Les objectifs peuvent avoir différents aspects et catégories, et peuvent concerner différents niveaux.

Note 3 à l'article : Un risque est généralement exprimé en termes de sources de risque, *événements* (3.16) potentiels, leurs *conséquences* (3.9) et leur *vraisemblance* (3.23).

[SOURCE : ISO 31000:2018, 3.1, modifiée.]

3.49
appréciation du risque
ensemble du *processus* (3.40) d'identification des risques, d'analyse du risque et d'évaluation du risque

Note 1 à l'article : L'appréciation du risque est décrite en détail dans l'ISO 31000:2018.

[SOURCE : ISO 22300:2018, 3.203 modifiée. La Note 1 à l'article a été modifiée.]

3.50
management du risque
activités (3.1) coordonnées dans le but de diriger et piloter un *organisme* (3.31) vis-à-vis du *risque* (3.48)

[SOURCE : ISO 31000:2018, 3.2]

3.51
chaîne d'approvisionnement
relation bilatérale entre *organismes* (3.31), personnes, *processus* (3.40), logistiques, *informations* (3.20), technologie et ressources engagés dans des *activités* (3.1) et créant de la valeur depuis l'approvisionnement en matières premières jusqu'à la délivrance de produits et de services

Note 1 à l'article : La chaîne d'approvisionnement peut comprendre divers fournisseurs, sous-traitants, installations de fabrication, fournisseurs de logistique, centres de distribution internes, distributeurs, grossistes et autres entités qui mènent à l'utilisateur final.

[SOURCE : ISO 22300:2018, 3.251, modifiée en « produits et de services ».]

3.52
test
type unique et particulier d'*exercice* (3.17) qui intègre l'attente d'un élément de réussite ou d'échec dans le but ou les *objectifs* (3.30) de l'exercice planifié

Note 1 à l'article : Les termes « test(s) » et « exercice(s) » ne sont pas identiques.

[SOURCE : ISO 22300:2018, 3.257, modifiée.]

3.53
direction
personne ou groupe de personnes qui oriente et dirige un *organisme* (3.31) au plus haut niveau

Note 1 à l'article : La direction a le pouvoir de déléguer son autorité et de fournir des ressources au sein de l'organisme.

Note 2 à l'article : Si le domaine d'application du *système de management* (3.25) ne couvre qu'une partie de l'organisme, alors la direction se réfère à ceux qui orientent et dirigent cette partie de l'organisme.

[SOURCE : ISO 22300:2018, 3.263, modifiée. Les Notes 3, 4 et 5 à l'article ont été supprimées.]

3.54
formation
activités (3.1) conçues pour faciliter l'apprentissage et le développement des connaissances, des compétences et des aptitudes et pour améliorer la *réalisation* (3.33) de tâches ou rôles spécifiques

[SOURCE : ISO 22300:2018, 3.265]

3.55
vérification
confirmation, par des preuves objectives, que les *exigences* (3.45) spécifiées ont été satisfaites

[SOURCE : ISO 22300:2018, 3.272]

3.56
environnement de travail
ensemble des conditions dans lesquelles un travail est effectué

Note 1 à l'article : Ces conditions peuvent intégrer des aspects physiques, sociaux, psychologiques et environnementaux (tels que température, éclairage, dispositifs de reconnaissance, stress professionnel, ergonomie et composition de l'atmosphère).

[SOURCE : ISO 22300:2018, 3.276]

4 Contexte de l'organisme

4.1 Compréhension de l'organisme et de son contexte

L'organisme doit déterminer les questions externes et internes pertinentes vis-à-vis de sa mission, et qui affectent son aptitude à obtenir le(s) résultat(s) attendu(s) de son SMCA.

NOTE Ces questions seront influencées par les objectifs globaux de l'organisme, ses produits et services et le niveau et le type de risque qu'il peut prendre ou non.

4.2 Compréhension des besoins et attentes des parties intéressées

4.2.1 Généralités

Lors de l'établissement de son SMCA, l'organisme doit déterminer :

a) les parties intéressées qui sont pertinentes pour le SMCA ;

b) les exigences de ces parties intéressées.

4.2.2 Exigences réglementaires et juridiques

L'organisme doit :

a) mettre en œuvre et maintenir un processus lui permettant d'identifier, d'avoir accès et d'apprécier les exigences réglementaires et juridiques concernant la continuité de ses produits et services, processus, activités et ressources, ainsi que les intérêts des parties intéressées pertinentes ;

b) s'assurer que les exigences réglementaires et juridiques ou autres, applicables, sont prises en compte lorsqu'il met en œuvre et maintient son SMCA ;

c) documenter ces informations et les tenir à jour.

4.3 Détermination du domaine d'application du système de management de la continuité d'activité

4.3.1 Généralités

Pour établir le domaine d'application du SMCA, l'organisme doit en déterminer les limites et l'applicabilité.

Lorsqu'il établit ce domaine d'application, il doit prendre en considération :

a) les questions externes et internes auxquelles il est fait référence en 4.1 ;

b) les exigences auxquelles il est fait référence en 4.2.

Le domaine d'application doit être disponible sous forme d'information documentée.

4.3.2 Domaine d'application du SMCA

L'organisme doit :

a) prendre en considération sa mission, ses buts et ses obligations internes et externes ;

b) établir les parties de l'organisme à inclure dans le SMCA, en prenant en compte leur(s) emplacement(s), taille, nature et complexité ;

c) identifier les produits et services et leurs processus, activités et ressources associés devant être inclus dans le SMCA ;

d) prendre en compte les besoins des parties intéressées.

Lors de la définition du domaine d'application, l'organisme doit documenter et expliquer les exclusions. De telles exclusions ne doivent pas affecter l'aptitude et la responsabilité de l'organisme à assurer la continuité de l'activité, tel que déterminé par le bilan d'impact sur l'activité ou l'appréciation du risque et par les exigences réglementaires ou juridiques applicables.

4.4 Système de management de la continuité d'activité

L'organisme doit établir, mettre en œuvre, maintenir et continuellement améliorer un SMCA, incluant les processus nécessaires et leurs interactions, en accord avec les exigences du présent document.

5 Leadership

5.1 Leadership et engagement

La Direction doit démontrer son leadership et son engagement en faveur du SMCA en :

a) s'assurant que la politique et les objectifs de continuité d'activité sont établis et qu'ils sont compatibles avec l'orientation stratégique de l'organisme ;

b) s'assurant que les exigences liées au SMCA sont intégrées aux processus métier de l'organisme ;

c) s'assurant que les ressources nécessaires pour le SMCA sont disponibles ;

d) communiquant sur l'importance d'une continuité d'activité efficace et (en) se conformant aux exigences liées au SMCA ;

e) s'assurant que le SMCA atteint le ou les résultats escomptés ;

f) orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du SMCA ;

g) aidant les autres managers pertinents à démontrer leur leadership et leur engagement dès lors que cela s'applique à leurs domaines de responsabilité ;

h) promouvant l'amélioration continue.

NOTE Dans le présent document, il est possible d'interpréter le terme « métier » au sens large, c'est-à-dire comme se référant aux activités liées à l'existence même de l'organisme.

5.2 Politique

5.2.1 La Direction doit établir une politique de continuité d'activité qui :

a) est appropriée à la mission de l'organisme ;

b) fournit un cadre pour l'établissement d'objectifs de continuité d'activité ;

c) inclut l'engagement de satisfaire aux exigences applicables ;

d) inclut l'engagement d'amélioration continue du SMCA.

5.2.2 La politique de continuité d'activité doit :

a) être disponible sous forme d'information documentée ;

b) être communiquée au sein de l'organisme ;

c) être à la disposition des parties intéressées, comme approprié.

5.3 Rôles, responsabilités et autorités au sein de l'organisme

La Direction doit s'assurer que les responsabilités et autorités pour les rôles pertinents sont attribuées et communiquées au sein de l'organisme.

La Direction doit désigner qui a la responsabilité et l'autorité de :

a) s'assurer que le SMCA est conforme aux exigences du présent document ;

b) rendre compte à la Direction des performances du SMCA.

6 Planification

6.1 Actions face aux risques et opportunités

Lorsqu'il conçoit son SMCA, l'organisme doit prendre en considération les questions auxquelles il est fait référence en 4.1 et les exigences auxquelles il est fait référence en 4.2 et déterminer les risques et opportunités auxquels il faut faire face pour :

a) fournir l'assurance que le système de management peut atteindre le ou les résultats escomptés ;

b) empêcher ou limiter les effets indésirables ; et

c) obtenir une démarche d'amélioration continue.

L'organisme doit planifier :

a) les actions à mener face aux risques et opportunités ;

b) la manière :

1) d'intégrer et de mettre en œuvre ces actions au sein des processus du SMCA (voir 8.1) ; et

2) d'évaluer l'efficacité de ces actions (voir 9.1).

NOTE Les risques et opportunités dans ce paragraphe se rapportent à l'efficacité du système de management. Les risques liés à une perturbation de l'activité sont traités en 8.2.

6.2 Objectifs de continuité d'activité et planification pour les atteindre

6.2.1 L'organisme doit établir les objectifs de continuité d'activité aux fonctions et niveaux pertinents.

Les objectifs de continuité d'activité doivent :

a) être cohérents avec la politique de continuité d'activité ;

b) être mesurables (si possible) ;

c) prendre en compte les exigences applicables ;

d) être surveillés ;

e) être communiqués ;

f) être mis à jour comme approprié.

L'organisme doit conserver des informations documentées sur les objectifs de continuité d'activité.

6.2.2 Lorsque l'organisme planifie la façon d'atteindre ses objectifs de continuité d'activité, l'organisme doit déterminer :

a) ce qui sera fait ;

b) quelles ressources seront requises ;

c) qui sera responsable ;

d) à quelle échéance ;

e) comment les résultats seront évalués.

6.3 Planification des modifications du SMCA

Lorsque l'organisme détermine le besoin d'apporter des modifications au SMCA, y compris celles identifiées à l'Article 10 sur l'amélioration, les modifications doivent être réalisées de façon planifiée.

L'organisme doit prendre en considération :

a) l'objet des modifications et leurs conséquences potentielles ;

b) l'intégrité du SMCA ;

c) la disponibilité des ressources ;

d) l'attribution ou la réattribution des responsabilités et autorités.

7 Support

7.1 Ressources

L'organisme doit déterminer et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la maintenance et l'amélioration continue du SMCA.

7.2 Compétences

L'organisme doit :

a) déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui affecte ses performances de continuité d'activité ;

b) s'assurer que ces personnes sont compétentes sur la base d'une formation initiale, d'une formation professionnelle ou d'une expérience appropriée ;

c) le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité des actions entreprises ;

d) conserver des informations documentées appropriées comme preuves de ces compétences.

NOTE Les actions envisageables peuvent par exemple inclure la formation, l'encadrement ou la réaffectation de personnes couramment employées ; ou le recrutement ou la mise sous contrat de personnes compétentes.

7.3 État de conscience

Les personnes effectuant un travail sous le contrôle de l'organisme doivent avoir conscience :

a) de la politique de continuité d'activité ;

b) de leur contribution à l'efficacité du SMCA, y compris les bénéfices d'une amélioration des performances de la continuité d'activité ;

c) des implications de la non-conformité aux exigences liées au SMCA ;

d) de leurs propres rôle et responsabilités, durant et après des perturbations.

7.4 Communication

L'organisme doit déterminer les éléments de communication interne et externe pertinents pour le SMCA, et notamment :

a) sur quelles questions communiquer ;

b) à quels moments communiquer ;

c) avec qui communiquer ;

d) comment communiquer ;

e) qui communiquera.

7.5 Informations documentées

7.5.1 Généralités

Le SMCA de l'organisme doit inclure :

a) les informations documentées exigées par le présent document ;

b) les informations documentées que l'organisme juge nécessaires à l'efficacité du SMCA.

NOTE L'étendue des informations documentées dans le cadre d'un SMCA peut différer selon l'organisme en fonction de :

la taille de l'organisme, ses types de produits et services, ses processus, activités et ressources ;

la complexité des processus et de leurs interactions ;

la compétence des personnes.

7.5.2 Création et mise à jour

Quand il crée et met à jour ses informations documentées, l'organisme doit s'assurer que sont appropriés :

a) l'identification et la description (par exemple titre, date, auteur, numéro de référence) ;

b) le format (par exemple langue, version logicielle, graphiques) et support (par exemple papier, électronique) ;

c) la revue et l'approbation du caractère adapté et adéquat des informations.

7.5.3 Maîtrise des informations documentées

7.5.3.1 Les informations documentées exigées par le SMCA et par le présent document doivent être maîtrisées pour s'assurer :

a) qu'elles sont disponibles et propres à être utilisées, où et quand c'est nécessaire ;

b) qu'elles sont convenablement protégées (par exemple de perte de confidentialité, utilisation inappropriée ou perte d'intégrité).

7.5.3.2 Pour maîtriser les informations documentées, l'organisme doit s'occuper des activités suivantes, quand elles lui sont applicables :

a) distribution, accès, récupération et utilisation ;

b) stockage et préservation, y compris préservation de la lisibilité ;

c) maîtrise des modifications (par exemple maîtrise des versions) ;

d) conservation et élimination des informations.

Les informations documentées d'origine externe que l'organisme juge nécessaires à la planification et au fonctionnement du SMCA doivent être identifiées comme approprié et maîtrisées.

NOTE L'accès peut impliquer une décision concernant l'autorisation de consulter les informations documentées uniquement, ou l'autorisation et l'autorité de consulter et modifier les informations documentées.

8 Fonctionnement

8.1 Planification opérationnelle et maîtrise

L'organisme doit planifier, mettre en œuvre et maîtriser les processus nécessaires à la satisfaction des exigences et à la réalisation des actions déterminées en 6.1, en :

a) établissant les critères pour ces processus ;

b) mettant en œuvre la maîtrise de ces processus en accord avec ces critères ;

c) conservant des informations documentées dans la mesure nécessaire pour avoir confiance que les processus ont été suivis comme prévu.

L'organisme doit maîtriser les modifications prévues, passer en revue les conséquences des modifications non intentionnelles et, si nécessaire, mener des actions pour limiter tout effet négatif.

L'organisme doit s'assurer que les processus externalisés et la chaîne d'approvisionnement sont maîtrisés.

8.2 Bilan d'impact sur l'activité et appréciation du risque

8.2.1 Généralités

L'organisme doit mettre en œuvre et maintenir un processus de bilan d'impact sur l'activité et d'appréciation du risque de perturbation qui établit le contexte, définit des critères et évalue l'impact potentiel d'une perturbation.

NOTE L'organisme détermine l'ordre dans lequel le bilan d'impact sur l'activité et l'appréciation du risque sont effectués.

8.2.2 Bilan d'impact sur l'activité

L'organisme doit mettre en œuvre et maintenir un processus pour déterminer les priorités et exigences de continuité d'activité qui :

a) définit les catégories d'impacts et les critères pertinents pour le contexte de l'organisme ;

b) utilise les catégories d'impacts et les critères pour mesurer les impacts ;

c) identifie les activités qui supportent la délivrance des produits et services ;

d) analyse les impacts dans le temps découlant de la perturbation de ces activités ;

e) identifie la durée au-delà de laquelle les impacts d'une non-reprise de ces activités deviendraient inacceptables pour l'organisme ;

NOTE Elle peut être appelée durée maximale tolérable de perturbation (DMTP).

f) détermine les délais par ordre de priorité à l'intérieur de la durée identifiée en e) ci-dessus pour reprendre les activités perturbées avec une capacité minimale acceptable spécifiée ;

NOTE Ils peuvent être désignés comme objectif de délai de rétablissement (RTO).

g) utilise les impacts sur l'activité pour identifier les activités prioritaires ;

h) détermine quelles ressources sont nécessaires pour soutenir les activités prioritaires ;

i) détermine les dépendances et interdépendances des activités prioritaires.

NOTE Les partenaires en externalisation peuvent être considérés selon l'ISO 22318.

8.2.3 Appréciation du risque

L'organisme doit mettre en œuvre et maintenir un processus d'appréciation du risque systématique.

NOTE Ce processus peut être réalisé selon l'ISO 31000.

L'organisme doit :

a) identifier les risques de perturbation pour les activités prioritaires de l'organisme, ainsi que pour les ressources qui les soutiennent ;

b) analyser les risques de perturbation de manière systématique ;

c) évaluer les risques de perturbation qui exigent un traitement.

NOTE Les risques dans ce paragraphe se rapportent à la perturbation de l'activité. Les risques et opportunités liés à l'efficacité du système de management sont traités en 6.1.

8.3 Stratégies et solutions de continuité d'activité

8.3.1 Généralités

L'organisme doit déterminer et sélectionner des stratégies de continuité d'activité se basant sur les éléments de sortie du bilan d'impact sur l'activité et de l'appréciation du risque. Les stratégies de continuité d'activité doivent comprendre une ou plusieurs solutions.

8.3.2 Identification et sélection des stratégies et solutions

L'organisme doit déterminer et sélectionner des stratégies et des solutions de continuité d'activité appropriées en prenant en considération leurs coûts associés pour :

a) répondre aux perturbations ;

b) continuer et rétablir les activités prioritaires et leurs ressources requises afin de satisfaire la délivrance de produits et services au niveau de capacité convenu dans le temps.

Pour les activités prioritaires, l'organisme doit déterminer et sélectionner des stratégies et solutions – en prenant en considération les objectifs de continuité d'activité et le niveau et le type de risque que l'organisme peut prendre ou non - qui :

a) réduisent la vraisemblance des perturbations ;

b) raccourcissent la période de perturbation ;

c) limitent l'impact de la perturbation sur les produits et services de l'organisme.

8.3.3 Exigences de ressources

L'organisme doit déterminer les exigences de ressources pour mettre en œuvre les solutions de continuité d'activité sélectionnées. Les types de ressources considérés doivent comprendre, sans toutefois s'y limiter :

a) les personnes ;

b) les informations et les données ;

c) l'infrastructure physique telle que les bâtiments, les lieux de travail ou d'autres installations et les utilités associées ;

d) les équipements et les consommables ;

e) les systèmes de technologies de l'information et de la communication (TIC) ;

f) le transport ;

g) le financement ;

h) les partenaires et fournisseurs.

8.3.4 Mise en œuvre des solutions

L'organisme doit mettre en œuvre les solutions de continuité d'activité sélectionnées afin qu'elles puissent être activées quand c'est nécessaire.

8.4 Plans et procédures de continuité d'activité

8.4.1 Généralités

L'organisme doit mettre en œuvre et maintenir une structure qui permettra d'avertir et communiquer en temps opportun avec les parties intéressées pertinentes, ainsi que fournir des plans et procédures pour gérer l'organisme lors d'une perturbation. Les plans et procédures doivent être utilisés quand c'est nécessaire pour exécuter les solutions de continuité d'activité.

NOTE Il existe différents types de procédures qui constituent les plans de continuité d'activité.

Les procédures doivent :

a) être précises concernant les mesures immédiates devant être prises pendant une perturbation ;

b) être souples pour répondre aux changements de conditions internes et externes d'une perturbation ;

c) se concentrer sur l'impact d'incidents menant potentiellement à une perturbation ;

d) être efficaces pour réduire l'impact au minimum par la mise en œuvre de solutions appropriées ;

e) attribuer des rôles et responsabilités pour les tâches qu'elles présentent.

8.4.2 Structure de réponse

L'organisme doit mettre en œuvre et maintenir une structure identifiant une ou plusieurs équipes chargées de répondre aux perturbations.

Les rôles et responsabilités de chaque équipe et les relations entre les équipes doivent être clairement établis.

Les équipes doivent être préparées collectivement à :

a) apprécier la nature et l'étendue d'une perturbation ainsi que son impact potentiel ;

b) apprécier l'impact par rapport aux seuils prédéfinis justifiant le lancement initial d'une réponse formelle ;

c) activer une réponse appropriée pour la continuité d'activité ;

d) planifier les actions à entreprendre ;

e) établir des priorités (en considérant la sécurité de la vie des personnes comme la première priorité) ;

f) surveiller les effets de la perturbation et la réponse de l'organisme ;

g) activer les solutions de continuité d'activité ;

h) communiquer avec les parties intéressées pertinentes, les autorités et les médias.

Chaque équipe doit avoir :

a) un personnel identifié et ses collaborateurs, avec la responsabilité, l'autorité et la compétence nécessaires pour exercer le rôle qui leur est attribué ;

b) des procédures documentées pour servir de guide à leurs actions (voir 8.4.4), y compris celles destinées à l'activation, au fonctionnement, à la coordination et à la communication de la réponse.

8.4.3 Avertissement et communication

8.4.3.1 L'organisme doit documenter et maintenir des procédures pour :

a) communiquer en interne et en externe avec les parties intéressées pertinentes, y compris quoi, quand, avec qui et comment communiquer ;

NOTE L'organisme peut documenter et maintenir des procédures concernant la manière et les circonstances dans lesquelles l'organisme communique avec les employés et les personnes à contacter en cas d'urgence.

b) gérer la réception, la documentation et la réponse aux communications provenant des parties intéressées, y compris un système de conseil national ou régional sur les risques ou un système équivalent ;

c) assurer la disponibilité des moyens de communication au cours d'une perturbation ;

d) faciliter une communication structurée avec les services d'urgence ;

e) les détails de la réponse de l'organisme aux médias à la suite d'un incident, y compris une stratégie de communication ;

f) effectuer l'enregistrement des détails de la perturbation, des actions réalisées et des décisions prises.

8.4.3.2 Le cas échéant, les éléments suivants doivent également être considérés et mis en œuvre :

a) alerter les parties intéressées potentiellement impactées par une perturbation réelle ou imminente ;

b) assurer une coordination et une communication appropriées entre de multiples organismes participant à la réponse.

Les procédures de communication et d'avertissement doivent faire l'objet d'exercices dans le cadre du programme d'exercices de l'organisme dont il est fait référence en 8.5.

8.4.4 Plans de continuité d'activité

8.4.4.1 Les plans de continuité d'activité doivent fournir des recommandations et des informations qui aideront les équipes à répondre à une perturbation et aideront l'organisme à répondre et à se rétablir.

Les plans de continuité d'activité doivent globalement contenir :

a) les détails des actions que les équipes accompliront afin de continuer ou de rétablir les activités prioritaires dans des délais prédéterminés et de surveiller les effets de la perturbation et la réponse de l'organisme à celle-ci ;

b) la référence au seuil prédéfini et au processus visant à activer la réponse ;

c) les procédures permettant la délivrance des produits et services au niveau de capacité convenu aux parties intéressées ;

d) les détails permettant de gérer les conséquences immédiates d'une perturbation en tenant dûment compte :

   1) du bien-être des individus ;

   2) de la prévention d'une perte ou indisponibilité supplémentaire d'activités prioritaires ;

   3) de la protection de l'environnement ;

e) un processus de sortie une fois que l'incident est terminé.

8.4.4.2 Chaque plan doit inclure :

a) le but, le domaine d'application et les objectifs ;

b) les rôles, les responsabilités de l'équipe qui mettra en œuvre le plan ;

c) les actions et ressources pour mettre en œuvre les solutions ;

d) les informations d'appui nécessaires pour activer (y compris les critères d'activation), mettre en œuvre, coordonner et communiquer les actions de l'équipe ;

e) les interdépendances internes et externes ;

f) les exigences de ressources ;

g) les exigences de compte rendu.

Chaque plan doit être utilisable et disponible au moment et à l'endroit auxquels il est requis.

8.4.5 Rétablissement

L'organisme doit disposer de processus documentés pour restaurer et revenir à ses activités métier à partir des mesures temporaires adoptées pour satisfaire aux exigences métier habituelles pendant et après une perturbation.

8.5 Programme d'exercices

L'organisme doit mettre en œuvre et maintenir un programme d'exercices et de tests afin de valider dans le temps l'efficacité de ses stratégies et solutions de continuité d'activité.

L'organisme doit mener des exercices et des tests qui :

a) sont cohérents avec ses objectifs de continuité d'activité ;

b) sont basés sur des scénarios appropriés qui sont bien planifiés avec des buts et des objectifs clairement définis ;

c) développent le travail d'équipe, les compétences, la confiance et les connaissances des personnes qui ont des rôles à jouer en lien avec les perturbations ;

d) cumulés au fil du temps, valident l'ensemble de ses stratégies de continuité d'activité ;

e) permettent de produire des rapports post-exercices formalisés contenant les résultats, les recommandations et les actions pour mettre en œuvre des améliorations ;

f) sont passés en revue dans le contexte de l'effort d'amélioration continue ;

g) sont menés à des intervalles planifiés et lorsque des changements significatifs interviennent au sein de l'organisme ou dans le contexte dans lequel il opère.

L'organisme doit agir en fonction des résultats de ses exercices et tests pour mettre en œuvre des modifications et améliorations.

9 Évaluation de la performance

9.1 Surveillance, mesurage, analyse et évaluation

9.1.1 Généralités

L'organisme doit déterminer :

a) ce qu'il est nécessaire de surveiller et mesurer ;

b) les méthodes de surveillance, de mesurage, d'analyse et d'évaluation, selon les cas, pour assurer la validité des résultats ;

c) quand et par qui la surveillance et le mesurage doivent être effectués ;

d) quand et par qui les résultats de la surveillance et du mesurage doivent être analysés et évalués.

L'organisme doit conserver des informations documentées appropriées comme preuves des résultats.

L'organisme doit évaluer les performances du SMCA et l'efficacité du SMCA.

9.1.2 Évaluation des plans, procédures et capacités de continuité d'activité

L'organisme doit évaluer l'adaptation, l'adéquation et l'efficacité de ses plans, procédures et capacités de continuité d'activité.

Ces évaluations doivent être réalisées par le biais de revues périodiques, d'analyses, d'exercices, de tests, de rapports post-incident et d'évaluations des performances.

L'organisme doit évaluer périodiquement la conformité aux exigences réglementaires et juridiques applicables, aux meilleures pratiques de son secteur ainsi que la conformité à sa propre politique de continuité d'activité et aux objectifs associés.

L'organisme doit réaliser les évaluations à des intervalles planifiés après un incident ou une activation et, lorsque des changements significatifs interviennent, celles-ci doivent être mises à jour en temps opportun.

9.2 Audit interne

9.2.1 L'organisme doit réaliser des audits internes à des intervalles planifiés afin de fournir des informations permettant de déterminer si le SMCA :

a) est conforme :

   1) aux exigences propres de l'organisme concernant son SMCA ;

   2) aux exigences du présent document ;

b) est efficacement mis en œuvre et maintenu.

9.2.1 L'organisme doit :

a) planifier, établir, mettre en œuvre et maintenir un (des) programme(s) d'audit, couvrant notamment la fréquence, les méthodes, les responsabilités, les exigences de planification et de comptes rendus. Le ou les programmes d'audit doivent prendre en considération l'importance des processus concernés et des résultats des audits précédents ;

b) définir les critères d'audit et le périmètre de chaque audit ;

c) sélectionner des auditeurs et réaliser des audits pour assurer l'objectivité et l'impartialité du processus d'audit ;

d) s'assurer qu'il est rendu compte des résultats des audits au management pertinent ;

e) conserver des informations documentées comme preuves de la mise en œuvre du programme d'audit et des résultats d'audit.

9.3 Revue de direction

9.3.1 Généralités

La Direction doit passer en revue le SMCA de l'organisme, à des intervalles planifiés afin de s'assurer qu'il est toujours adapté, adéquat et efficace.

9.3.2 Éléments d'entrée de la revue de direction

La revue de direction doit prendre en considération :

a) l'état d'avancement des actions décidées lors des revues de direction précédentes ;

b) les modifications des questions externes et internes pertinentes pour le SMCA ;

c) les informations sur les performances de continuité d'activité, y compris les tendances concernant :

   1) les non-conformités et les actions correctives ;

   2) les résultats de l'évaluation de la surveillance et du mesurage ;

   3) les résultats des audits ;

d) les retours d'information des parties intéressées ;

e) le besoin d'apporter des modifications au SMCA, y compris la politique et les objectifs ;

f) les procédures et les ressources qui pourraient être utilisées dans l'organisme pour améliorer les performances et l'efficacité du SMCA ;

g) les informations issues du bilan d'impact sur l'activité et de l'appréciation du risque ;

h) les risques ou les questions qui n'ont pas été traités de manière adéquate lors d'une précédente appréciation des risques ;

i) les résultats des exercices et des tests ;

j) les leçons tirées et les actions découlant d'incidents évités de justesse et de perturbations ;

k) les opportunités pour l'amélioration continue.

9.3.3 Éléments de sortie de la revue de direction

9.3.3.1 Les éléments de sortie de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et au possible besoin d'apporter des modifications au SMCA pour améliorer son efficience et son efficacité ; elles doivent inclure les éléments suivants :

a) les variations apportées au domaine d'application du SMCA ;

b) la mise à jour du bilan d'impact sur l'activité, de l'appréciation du risque, des stratégies et solutions de continuité d'activité et des plans de continuité d'activité ;

c) la modification des procédures et des moyens de maîtrise pour répondre aux questions internes ou externes qui peuvent impacter le SMCA ;

d) la manière dont l'efficacité des moyens de maîtrise sera mesurée.

9.3.3.2 L'organisme doit conserver des informations documentées comme preuve des résultats des revues de direction, et :

a) communiquer les résultats de la revue de direction aux parties intéressées pertinentes ;

b) entreprendre l'action appropriée en fonction de ces résultats.

10 Amélioration

10.1 Non-conformité et actions correctives

10.1.1 Lorsqu'une non-conformité se produit, l'organisme doit :

a) réagir à la non-conformité, et le cas échéant :

   1) agir pour la maîtriser et la corriger ;

   2) faire face aux conséquences ;

b) évaluer le besoin d'agir pour éliminer les causes de la non-conformité, de sorte qu'elle ne se reproduise pas ni ne se reproduise ailleurs, en :

   1) passant en revue la non-conformité ;

   2) déterminant les causes de la non-conformité ;

   3) déterminant si des non-conformités similaires existent, ou pourraient potentiellement se produire ;

c) mettre en œuvre toute action nécessaire ;

d) passer en revue l'efficacité de toute action corrective mise en œuvre ;

e) modifier, si nécessaire, le SMCA.

Les actions correctives doivent être appropriées aux effets des non-conformités rencontrées.

10.1.2 L'organisme doit conserver des informations documentées comme preuves :

a) de la nature des non-conformités et de toutes les actions menées ultérieurement ;

b) des résultats de toute action corrective.

10.2 Amélioration continue

L'organisme doit continuellement améliorer l'adaptation, l'adéquation et l'efficacité du SMCA.

L'organisme doit prendre en considération les résultats de l'analyse et de l'évaluation, ainsi que les éléments de sortie de la revue de direction pour déterminer s'il existe des besoins ou des opportunités à considérer dans le cadre de l'amélioration continue.

NOTE L'organisme peut utiliser les processus du SMCA tels que le leadership, la planification et l'évaluation de la performance, afin d'obtenir une amélioration.

Bibliographie

[1] ISO 9001, *Systèmes de management de la qualité — Exigences*

[2] ISO 14001, *Systèmes de management environnemental — Exigences et lignes directrices pour son utilisation*

[3] ISO 19011, *Lignes directrices pour l'audit des systèmes de management*

[4] ISO/IEC/TS 17021-6, *Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management — Partie 6 : Exigences de compétence pour l'audit et la certification des systèmes de management de la continuité d'activité*

[5] ISO/IEC 20000-1, *Technologies de l'information — Gestion des services — Partie 1 : Exigences du système de management des services*

[6] ISO 22300, *Sécurité et résilience — Vocabulaire*

[7] ISO/IEC 27001, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

[8] ISO/IEC 27031, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité*

[9] ISO 28000, *Spécifications relatives aux systèmes de management de la sûreté de la chaîne d'approvisionnement*

[10] ISO 31000, *Management du risque — Lignes directrices*

[11] ISO/IEC 31010, *Gestion des risques — Techniques d'évaluation des risques*

[12] SI 24001, *Security and continuity management systems — Requirements and guidance for use*, Standards Institution of Israel

[13] NFPA 1600, *Standard on disaster/emergency management and business continuity programs, National Fire Protection Association (USA)*

[14] *Business Continuity Plan Drafting Guideline*. Ministry of Economy, Trade and Industry, Japan, 2005

[15] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[16] ANSI/ASIS SPC. – 2011, Auditing management systems: Risk, *Resilience: Security, and Continuity –Guidance for Application*

[17] ANSI/ASIS/BSI BCM.01, *Business Continuity Management Systems: Requirements with Guidance for Use*