ISO/TC 223/SC

Date: 2012-05-15

ISO 22301:2012(F)

ISO/TC 223/SC /GT

Secrétariat: SIS

Sécurité sociétale — Gestion de la continuité d'activité — Exigences

Societal security — Business continuity management systems — Requirements

Type du document: Norme internationale
Sous-type du document:
Stade du document: (60) Publication
Langue du document: F

STD Version 2.4a

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*.

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 pour les systèmes de management de la sûreté pour 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.

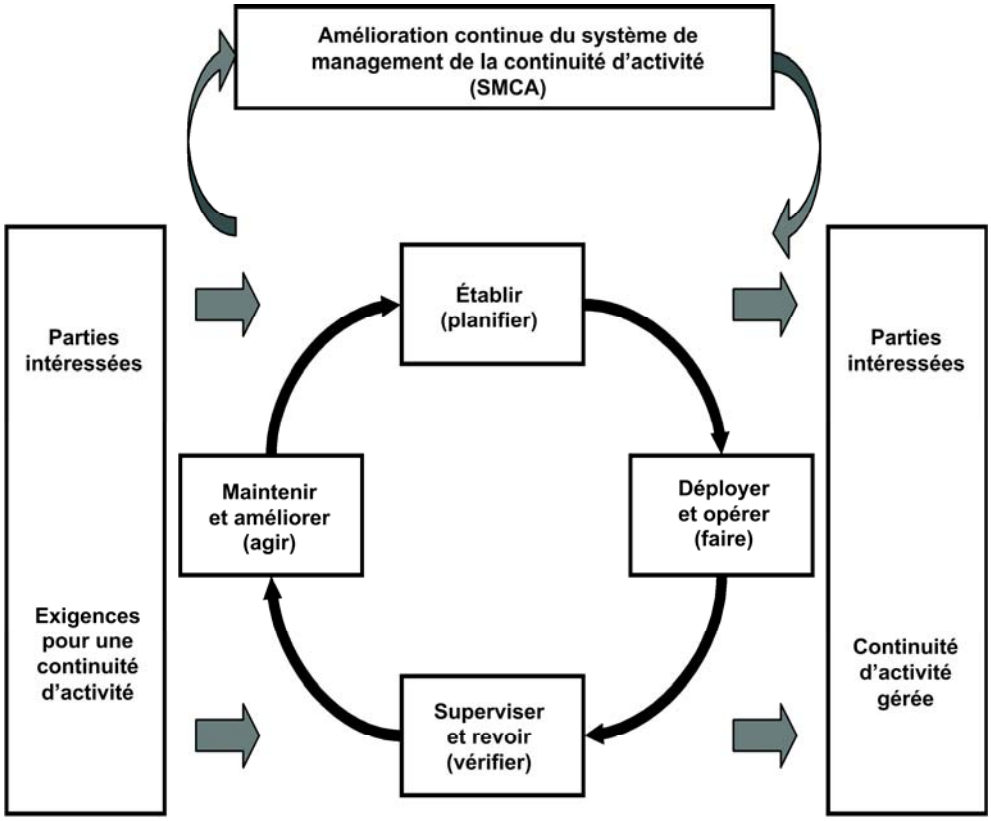

Figure 1 — Modèle PDCA appliqué aux processus d'un SMCA

Tableau 1 — Explication du modèle PDCA

Planifier (Etablir)	Etablir 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 Eléments 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 — Gestion 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

3.21
partie intéressée
partie prenante
personne ou organisation qui peut avoir une incidence sur, être affectée ou se sentir affectée par une décision ou une activité

NOTE Il peut s'agir d'un individu ou d'un groupe ayant un intérêt dans les décisions ou activités d'une organisation.

3.22
audit interne
audit réalisé par, ou pour le compte de, l'organisation elle-même pour la revue de direction et d'autres besoins internes et qui peut servir de base à l'autodéclaration de conformité de l'organisation

NOTE Dans de nombreux cas et en particulier pour les petites organisations, l'indépendance peut être démontrée par l'absence de responsabilité vis-à-vis de l'activité à auditer.

3.23
déclenchement
acte consistant à déclarer que les dispositions en matière de continuité d'activité d'une organisation doivent être mises en œuvre afin de poursuivre la livraison de produits clés ou la prestation de services clés

3.24
système de management
ensemble d'éléments corrélés ou interactifs d'une organisation, utilisés pour établir des politiques et des objectifs, et de processus pour atteindre ces objectifs

NOTE 1 Un système de management peut concerner une seule ou plusieurs disciplines.

NOTE 2 Les éléments du système comprennent la structure organisationnelle, les rôles et responsabilités, la planification, le fonctionnement, etc.

NOTE 3 Le périmètre d'un système de management peut comprendre l'ensemble de l'organisation, des fonctions spécifiques et identifiées de l'organisation, des sections spécifiques et identifiées de l'organisation, ou une ou plusieurs fonctions dans un groupe d'organisations.

3.25
durée maximale d'interruption acceptable
DMIA (en anglais : MAO Maximum Acceptable Outage)
temps nécessaire pour que les impacts défavorables pouvant résulter de la non fourniture d'un produit/service ou de la non réalisation d'une activité, deviennent inacceptables

NOTE Voir aussi « durée maximale tolérable de perturbation ».

3.26
durée maximale tolérable de perturbation
DMTP (en anglais : MTPD Maximum Tolerable Period of Disruption)
temps nécessaire pour que les impacts défavorables pouvant résulter de la non fourniture d'un produit/service ou de la non réalisation d'une activité, deviennent inacceptables

NOTE Voir aussi « durée maximale d'interruption acceptable ».

3.27
mesurage
processus visant à déterminer une valeur

3.28
objectif minimal de continuité d'activité
OMCA (en anglais : MBCO Minimum Business Continuity Objective)
niveau minimal de services et/ou de produits acceptable par l'organisation pour atteindre ses objectifs métier pendant une perturbation

3.29
supervision
détermination de l'état d'un système, d'un processus ou d'une activité

NOTE Pour déterminer cet état, il peut être nécessaire de vérifier, surveiller ou observer avec une vision critique.

3.30
accord d'entraide mutuel
entente préalable entre deux entités ou plus par laquelle chacune d'elles s'engage à fournir assistance aux autres

[SOURCE : ISO 22300]

3.31
non-conformité
non-satisfaction d'une exigence

[SOURCE : ISO 22300]

3.32
objectif
résultat à atteindre

NOTE 1 Un objectif peut être stratégique, tactique ou opérationnel.

NOTE 2 Les objectifs peuvent se rapporter à différentes disciplines (telles que la finance, les enjeux sanitaires et de sécurité, et les enjeux environnementaux) et ils peuvent s'appliquer à divers niveaux [tels que stratégie, organisation dans son ensemble, projet, produit et processus].

NOTE 3 Un objectif peut être exprimé autrement, par exemple sous forme de résultat escompté, de mission, de critère opérationnel, en tant qu'objectif de sécurité sociétale ou par le biais d'un autre terme ayant un sens similaire (par exemple finalité, but, cible).

NOTE 4 Dans le contexte des normes de systèmes de management de la sécurité sociétale, les objectifs encadrés par la norme sont établis par l'organisation, en cohérence avec sa politique de sécurité sociétale, en vue d'obtenir des résultats spécifiques.

3.33
organisation
personne ou groupe de personnes ayant leur propre structure fonctionnelle avec des responsabilités, autorités et relations en vue d'atteindre ses objectifs

NOTE 1 Le concept d'organisation comprend, sans s'y limiter, les notions de travailleur indépendant, compagnie, société, firme, entreprise, autorité, groupement, organisation caritative ou institution, ou une partie ou une combinaison des organisations précédentes, à responsabilité limitée ou sous un autre statut, de droit public ou privé.

NOTE 2 Pour les organisations ayant plusieurs unités d'exploitation, une seule unité d'exploitation peut être définie en tant qu'organisation.

3.34
externaliser
passer un accord en vertu duquel une organisation externe effectue une partie de la fonction ou met en œuvre une partie du processus de l'organisation

NOTE L'organisation externe n'est pas incluse dans le périmètre du système de management, contrairement à la fonction ou au processus externalisé qui en fait bien partie.

3.35
performance
résultat mesurable

NOTE 1 La performance peut porter sur des constatations quantitatives ou qualitatives.

NOTE 2 La performance peut concerner le management d'activités, de processus, de produits (y compris services), de systèmes ou d'organisations.

3.36
évaluation de la performance
processus visant à déterminer des résultats mesurables

3.37
personnel
personnes travaillant pour l'organisation et sous le contrôle de celle-ci

NOTE Le concept de personnel inclut, sans toutefois s'y limiter, les employés, le personnel à temps partiel et le personnel intérimaire.

3.38
politique
intentions et orientations d'une organisation, telles qu'elles sont officiellement formulées par sa direction

3.39
procédure
manière spécifiée d'effectuer une activité ou un processus

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

3.41
produits et services
résultats fournis par une organisation au bénéfice de ses clients, ses destinataires et les parties intéressées (par exemple des articles manufacturés, une assurance automobile et des soins infirmiers communautaires)

3.42
activités prioritaires
activités auxquelles priorité doit être donnée à la suite d'un incident afin d'en atténuer les impacts

NOTE Les termes couramment utilisés pour décrire les activités de ce groupe comprennent : critiques, essentielles, vitales, urgentes et clés.

[SOURCE : ISO 22300]

3.43
enregistrement
déclaration des résultats obtenus ou preuves des activités réalisées

3.44
point de récupération des données
RPO
Point à partie duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement à la reprise

NOTE Il peut également être désigné en tant que « perte maximale de données ».

3.45
objectif de délai de reprise
RTO
durée après un incident durant laquelle :

— un produit ou un service doit être repris, ou

— une activité doit être reprise, ou

— des ressources doivent être rétablies

NOTE Pour les produits, les services et les activités, l'objectif de délai de reprise doit être inférieur au temps qu'il faudrait pour que les impacts défavorables qui résulteraient du défaut de fourniture d'un produit/service ou de l'absence de réalisation d'une activité, deviennent inacceptables.

3.46
exigence
besoin ou attente qui est formulé, généralement implicite ou obligatoire

NOTE 1 « Généralement implicite » signifie qu'il est habituel ou de pratique courante pour l'organisation et les parties intéressées que le besoin ou l'attente à prendre en considération soit implicite.

NOTE 2 Une exigence spécifiée est une exigence établie, par exemple dans une information documentée.

3.47
ressources
ensemble des biens, du personnel, des compétences, des informations, de la technologie (y compris l'usine et ses équipements), des locaux et des fournitures et informations (qu'elles soient électroniques ou non) dont doit disposer une organisation, au moment requis, pour fonctionner et atteindre son objectif

3.48
risque
effet de l'incertitude sur l'atteinte des objectifs

NOTE 1 Un effet est un écart, positif ou négatif, par rapport à une attente.

NOTE 2 Les objectifs peuvent avoir différents aspects (par exemple enjeux financiers, sanitaires et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (stratégie, projet, produit et processus ou organisation toute entière). Un objectif peut être exprimé autrement, par exemple sous forme de résultat escompté, de mission ou de critère opérationnel, en tant qu'objectif de continuité d'activité ou par le biais d'un autre terme ayant un sens similaire (par exemple finalité, but, cible).

NOTE 3 Un risque est souvent caractérisé en référence à des événements potentiels (Guide ISO 73, 3.5.1.3) et des conséquences potentielles (Guide ISO 73, 3.6.1.3) ou à une combinaison des deux.

NOTE 4 Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (y compris des changements de circonstances) et de sa vraisemblance (Guide ISO 73, 3.6.1.1).

NOTE 5 L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

NOTE 6 Dans le contexte des normes de systèmes de management de la continuité d'activité, les objectifs de continuité d'activité sont fixés par l'organisation, en cohérence avec sa politique de continuité d'activité, en vue d'atteindre des résultats spécifiques. Lorsque les termes « management du risque et des composantes du risque » s'appliquent, il convient de l'associer aux objectifs de l'organisation qui comprennent, sans toutefois s'y limiter, les objectifs de continuité d'activité spécifiés en 6.2.

[SOURCE : ISO/CEI Guide 73]

3.49
appétence au risque
niveau et type de risque qu'une organisation est prête à accepter

3.50
appréciation du risque
ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque

[SOURCE : ISO Guide 73]

3.51
management du risque
activités coordonnées dans le but de diriger et piloter une organisation vis-à-vis du risque

[SOURCE : ISO Guide 73]

3.52
test
méthode d'évaluation ; moyen de déterminer la présence, la qualité ou la véracité de quelque chose

NOTE 1 Les tests peuvent se référer à un « essai ».

NOTE 2 Les tests sont souvent appliqués à des plans de continuité.

[SOURCE : ISO 22300]

3.53
direction
personne ou groupe de personnes qui dirige et contrôle une organisation au plus haut niveau

NOTE 1 La direction a le pouvoir de déléguer son autorité et de fournir des ressources au sein de l'organisation.

NOTE 2 Si le périmètre du système de management couvre uniquement une partie de l'organisation, alors la direction se réfère à ceux qui dirigent et contrôlent cette partie de l'organisation.

3.54
vérification
confirmation, par des preuves, que les exigences spécifiées ont été satisfaites

3.55
environnement de travail
ensemble des conditions dans lesquelles un travail est effectué

NOTE Les conditions comprennent des facteurs physiques, sociaux, psychologiques et environnementaux (tels que la température, les systèmes de reconnaissance, l'ergonomie et la composition de l'air).

[SOURCE : ISO 22300]

4 Contexte de l'organisation

4.1 Compréhension de l'organisation et de son contexte

L'organisation doit déterminer les enjeux externes et internes pertinents vis-à-vis de sa mission, et qui influent sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son SMCA.

Ces enjeux doivent être pris en compte lors de l'établissement, de la mise en œuvre et du maintien du SMCA de l'organisation.

L'organisation doit identifier et documenter les éléments suivants :

a) les activités de l'organisation, ses fonctions, ses services, ses produits, ses partenariats, les chaînes d'approvisionnement, ses relations avec les parties intéressées, et l'impact potentiel lié à un incident perturbateur ;

b) les liens entre la politique de continuité d'activité et les objectifs de l'organisation ainsi que les autres politiques, y compris sa stratégie globale de management du risque ; et

c) l'appétence au risque de l'organisation.

Lors de l'établissement du contexte, l'organisation doit :

1) exprimer clairement ses objectifs, y compris ceux liés à la continuité d'activité ;

2) définir les facteurs externes et internes à l'origine de l'incertitude qui engendre un risque ;

3) établir les critères de risque en prenant en compte le goût du risque ; et

4) définir la finalité du SMCA.

4.2 Compréhension des besoins et attentes des parties intéressées

4.2.1 Généralités

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

a) les parties intéressées qui sont concernées par le SMCA ; et

b) les exigences de ces parties intéressées (c'est-à-dire leurs besoins et leurs attentes, que ceux-ci soient formulés, généralement de manière implicite, ou obligatoires).

4.2.2 Exigences légales et réglementaires

L'organisation doit établir, mettre en œuvre et tenir à jour une (des) procédure(s) lui permettant d'identifier, d'avoir accès et d'évaluer les exigences légales et réglementaires applicables auxquelles elle se soumet, en ce qui concerne la continuité de ses opérations, produits et services, ainsi que les intérêts des parties intéressées concernées.

L'organisation doit s'assurer que les exigences légales, réglementaires ou toutes autres en vigueur auxquelles elle est soumise sont prises en compte lorsqu'elle établit, met en œuvre et tient à jour son SMCA.

L'organisation doit documenter ces informations et les tenir à jour. Toute nouveauté ou modification des exigences légales et réglementaires et des autres exigences doit être communiquée aux employés concernés et à toutes les autres parties intéressées.

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'organisation doit en déterminer les limites et l'applicabilité.

Lorsqu'elle établit ce domaine d'application, l'organisation doit prendre en compte :

— les enjeux externes et internes auxquels il est fait référence en 4.1 ; et

— les exigences auxquelles il est fait référence en 4.2.

Le périmètre doit être disponible sous forme d'information documentée.

4.3.2 Domaine d'application du SMCA

L'organisation doit :

a) déterminer les parties de l'organisation à inclure dans le SMCA ;

b) définir les exigences relatives au SMCA, compte tenu de la mission de l'organisation, de ses buts, de ses obligations internes et externes (y compris celles liées aux parties intéressées) et de ses responsabilités légales et réglementaires ;

c) identifier les produits, les services et toutes activités associées entrant dans le domaine d'application du SMCA ;

d) prendre en compte les besoins et les intérêts des parties intéressées, tels que les clients, les investisseurs, les actionnaires, la chaîne d'approvisionnement, les suggestions et besoins, les attentes et les intérêts du public et/ou de la communauté (lorsque nécessaire) ; et

e) définir le domaine d'application du SMCA en termes et en fonction de la taille, de la nature et de la complexité de l'organisation.

Lors de la définition du domaine d'application, l'organisation doit documenter et expliquer les exclusions. De telles exclusions ne doivent pas affecter la capacité et la responsabilité de l'organisation à assurer la continuité de l'activité et des opérations conformément d'une part aux exigences du SMCA, telles que déterminées par l'analyse des impacts sur l'activité ou l'appréciation du risque, et d'autre part aux exigences légales ou réglementaires applicables.

4.4 Système de management de la continuité d'activité

L'organisation doit établir, mettre en œuvre, tenir à jour et continuellement améliorer un SMCA, y compris les processus nécessaires et leurs interactions, conformément aux exigences de la présente Norme internationale.

5 Leadership

5.1 Leadership et engagement

Les membres de la Direction et les autres managers concernés au sein de l'organisation doivent faire preuve de leadership en ce qui concerne le SMCA.

EXEMPLE Ce leadership et cet engagement peuvent être démontrés en incitant et en responsabilisant les personnes pour qu'elles contribuent à l'efficacité du SMCA.

5.2 Engagement de la direction

La direction doit faire preuve de leadership et affirmer son engagement en faveur du SMCA en :

— s'assurant que des politiques et des objectifs du SMCA sont établis et sont compatibles avec l'orientation stratégique de l'organisation ;

— s'assurant que les exigences liées au système de management de la continuité d'activité sont intégrées aux processus métier de l'organisation ;

— s'assurant que les ressources nécessaires pour le système de management de la continuité d'activité sont disponibles ;

— communiquant sur l'importance de disposer d'un système de management de la continuité d'activité efficace et de se conformer aux exigences liées à ce système ;

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

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

— promouvant l'amélioration continue ; et

— aidant les autres managers concernés à faire également preuve de leadership et d'engagement dès lors que cela s'applique à leurs domaines de responsabilité.

NOTE 1 Dans la présente Norme internationale, il convient d'interpréter le terme « métier » au sens large, c'est-à-dire comme se référant aux activités liées à l'existence même de l'organisation.

La direction doit fournir des preuves de son engagement en faveur de l'établissement, de la mise en œuvre, de l'exploitation, de la surveillance, de la revue, de la tenue à jour et de l'amélioration du SMCA en :

— établissant une politique de continuité d'activité ;

— s'assurant que les objectifs et les plans du SMCA sont établis ;

— établissant les rôles, les responsabilités et les compétences en matière de management de la continuité d'activité ; et

— désignant une ou plusieurs personnes en tant que responsables du SMCA, ces personnes ayant l'autorité et les compétences appropriées pour assumer la responsabilité de la mise en œuvre et de la mise à jour du SMCA.

NOTE 2 Ces personnes peuvent assumer d'autres responsabilités au sein de l'organisation.

La Direction doit s'assurer que les responsabilités et autorités des autres managers concernés sont attribuées et communiquées au sein de l'organisation en :

— définissant les critères d'acceptation des risques et les niveaux de risque acceptables ;

— s'engageant activement dans des exercices et des tests ;

— s'assurant que des audits internes du SMCA sont menés ;

— menant des revues de direction du SMCA ; et

— démontrant son engagement à œuvrer pour l'amélioration continue.

5.3 Politique

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

a) est adaptée à la mission de l'organisation ;

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'œuvrer pour l'amélioration continue du SMCA.

La politique du SMCA doit :

— être disponible sous forme d'information documentée ;

— être communiquée au sein de l'organisation ;

— être mise à la disposition des parties intéressées, le cas échéant ;

— faire l'objet d'une revue, à des intervalles définis et en cas de modifications significatives, afin de s'assurer qu'elle est toujours appropriée.

L'organisation doit conserver des informations documentées sur la politique de continuité d'activité.

5.4 Rôles, responsabilités et autorités au sein de l'organisation

La Direction doit s'assurer que les responsabilités et autorités des autres managers concernés sont attribuées et communiquées au sein de l'organisation.

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

a) s'assurer que le système de management est conforme aux exigences de la présente Norme internationale ; et

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

6 Planification

6.1 Actions face aux risques et opportunités

Lorsqu'elle conçoit son SMCA, l'organisation doit tenir compte des enjeux auxquels il est fait référence au paragraphe 4.1 et des exigences du paragraphe 4.2 et déterminer les risques et opportunités qui nécessitent d'être abordés pour :

a) s'assurer que le système de management peut atteindre le ou les résultats escomptés ;

b) empêcher ou limiter les effets indésirables ; et

c) appliquer une démarche d'amélioration continue ;

L'organisation doit planifier :

a) les actions menées du fait des 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).

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

La direction doit s'assurer que les objectifs de continuité d'activité sont établis et communiqués aux fonctions et niveaux concernés au sein de l'organisation.

Les objectifs de continuité d'activité doivent :

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

b) tenir compte du niveau minimal de fourniture de produits et services acceptable pour que l'organisation atteigne ses objectifs ;

c) être mesurables ;

d) tenir compte des exigences applicables ; et

e) être surveillés et mis à jour quand c'est nécessaire.

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

Pour atteindre ses objectifs de continuité d'activité, l'organisation doit déterminer :

— qui sera responsable ;

— ce qui sera fait ;

— les ressources qui seront nécessaires ;

— les échéances ; et

— la façon dont les résultats seront évalués.

7 Support

7.1 Ressources

L'organisation doit identifier et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la mise à jour et l'amélioration continue du SMCA.

7.2 Compétences

L'organisation doit :

a) déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur ses performances ;

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

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 notamment inclure la formation, l'encadrement ou la réaffectation du personnel actuellement employé ; le recrutement ou la signature d'un contrat avec des personnes compétentes.

7.3 Sensibilisation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent :

a) être sensibilisées à la politique de continuité d'activité ;

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

c) avoir conscience des implications de toute non-conformité aux exigences requises par le SMCA ; et

d) avoir conscience de leur propre rôle durant des incidents perturbateurs.

7.4 Communication

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

a) sur quels sujets communiquer ;

b) à quels moments communiquer ;

c) avec qui communiquer.

L'organisation doit établir, mettre en œuvre et tenir à jour une ou des procédures pour :

— la communication interne entre les parties intéressées et les employés au sein de l'organisation ;

— la communication externe avec les clients, les entités partenaires, les collectivités locales et les autres parties intéressées, y compris les médias ;

— la réception, la documentation et la réponse à une communication émanant de parties intéressées ;

— l'adaptation et l'intégration d'un système consultatif national ou régional sur les menaces, ou d'un système équivalent, dans la planification et l'exploitation, le cas échéant ;

— la garantie d'une disponibilité des moyens de communication au cours d'un incident perturbateur ;

— la facilitation d'une communication structurée avec les autorités appropriées et l'assurance de l'interopérabilité des multiples organismes et personnel d'intervention, le cas échéant ; et

— le fonctionnement et les tests des capacités de communication devant être utilisés pendant une perturbation des communications normales.

NOTE D'autres exigences relatives à la communication en réponse à un incident sont spécifiées en 8.4.3.

7.5 Informations documentées

7.5.1 Généralités

Le SMCA de l'organisation doit inclure :

— les informations documentées exigées par la présente Norme internationale ; et

— les informations documentées que l'organisation juge nécessaires à l'efficacité du SMCA.

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

— la taille de l'organisation, ses domaines d'activité et ses processus, produits et services ;

— la complexité des processus et de leurs interactions ; et

— la compétence des personnes.

7.5.2 Création et mise à jour

Quand elle crée et met à jour ses informations documentées, l'organisation doit s'assurer que les éléments suivants sont appropriés :

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

b) format (par exemple langue, version logicielle, graphiques), support (par exemple papier, électronique), et revue et validation du caractère approprié et adéquat des informations.

7.5.3 Maîtrise des informations documentées

Les informations documentées exigées par le SMCA et par la présente Norme internationale doivent être maîtrisées pour s'assurer :

a) qu'elles sont disponibles et propres à l'usage, où et quand elles sont nécessaires ;

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

Pour maîtriser les informations documentées, l'organisation doit s'intéresser aux activités suivantes, quand elles lui sont applicables :

— distribution, accès, récupération et utilisation ;

— stockage et conservation, y compris préservation de la lisibilité ;

— maîtrise des modifications (par exemple, contrôle des versions) ;

— durée de conservation et suppression des informations ;

— extraction et utilisation ;

— préservation de la lisibilité (c'est-à-dire suffisamment claires pour être lues) ; et

— prévention de l'usage involontaire d'informations obsolètes.

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

Lorsque l'organisation met en place la maîtrise des informations documentées, elle doit s'assurer de l'existence d'une protection adéquate des informations documentées (par exemple protection contre la compromission, la modification non autorisée ou la suppression).

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

8 Fonctionnement

8.1 Planification opérationnelle et maîtrise

L'organisation 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 des critères pour ces processus ;

b) mettant en œuvre la maîtrise de ces processus conformément aux critères ; et

c) conservant des informations documentées dans une mesure suffisante pour avoir l'assurance que les processus ont été suivis comme prévu.

L'organisation doit maîtriser les modifications prévues, analyser les conséquences des modifications imprévues et, si nécessaire, mener des actions pour limiter tout effet négatif.

L'organisation doit s'assurer que les processus externalisés sont maîtrisés.

8.2 Analyse des impacts sur l'activité et appréciation du risque

8.2.1 Généralités

L'organisation doit établir, mettre en œuvre et tenir à jour un processus formel et documenté d'analyse des impacts sur l'activité et d'appréciation du risque qui :

a) établit le contexte de l'appréciation, définit des critères et évalue l'impact potentiel d'un incident perturbateur ;

b) tient compte des exigences légales et de toutes les autres exigences auxquelles l'organisation se soumet ;

c) comprend une analyse systématique, l'établissement de priorités dans les traitements du risque et leurs coûts associés ;

d) définit le résultat requis de l'analyse des impacts sur l'activité et de l'appréciation du risque ; et

e) spécifie les exigences de mise à jour et de confidentialité de ces informations.

NOTE Il existe différentes méthodes d'analyse des impacts sur l'activité et d'appréciation du risque qui détermineront l'ordre dans lequel elles seront effectuées.

8.2.2 Analyse des impacts sur l'activité

L'organisation doit définir, mettre en œuvre et tenir à jour un processus d'évaluation formel et documenté permettant de déterminer les priorités, les objectifs et les cibles de continuité d'activité et de reprise. Ce processus doit comprendre l'évaluation des impacts d'une perturbation des activités de support à la fourniture des produits et des services de l'organisation.

L'analyse des impacts sur l'activité doit comprendre les éléments suivants :

a) identification des activités de support à la fourniture de produits et à la prestation de services ;

b) évaluation des impacts dans le temps en cas de non réalisation de ces activités ;

c) détermination des délais, par ordre de priorité, de reprise de ces activités à un niveau minimal acceptable spécifié, en tenant compte de la durée au-delà de laquelle les impacts d'une absence de reprise de ces activités deviendraient inacceptables ; et

d) identification des dépendances et des ressources de support de ces activités, y compris les fournisseurs, les partenaires externes et les autres parties intéressées concernées.

8.2.3 Appréciation du risque

L'organisation doit établir, mettre en œuvre et tenir à jour un processus formel et documenté d'appréciation du risque qui identifie, analyse et évalue de manière systématique le risque d'incidents perturbateurs pour l'organisation.

NOTE Ce processus peut être établi conformément à l'ISO 31000.

L'organisation doit :

a) identifier les risques de perturbation pour les activités prioritaires de l'organisation, ainsi que pour les processus, les systèmes, les informations, les personnes, les biens, les partenaires externes et les autres ressources qui les soutiennent ;

b) analyser le risque de manière systématique ;

c) évaluer les risques liés à une perturbation qui nécessitent un traitement ; et

d) identifier les traitements proportionnés aux objectifs de continuité d'activité et à l'appétence au risque de l'organisation.

NOTE L'organisation doit avoir conscience que certaines obligations financières et gouvernementales exigent la communication de ces risques à divers niveaux de détail. De plus, certains besoins sociétaux peuvent également justifier un partage de ces informations à un niveau de détail approprié.

8.3 Stratégie de continuité d'activité

8.3.1 Détermination et choix

La détermination et le choix d'une stratégie doivent être basés sur les conclusions de l'analyse d'impact sur l'activité et de l'appréciation du risque.

L'organisation doit déterminer une stratégie de continuité d'activité appropriée pour :

a) protéger les activités prioritaires ;

b) stabiliser, poursuivre, reprendre ou rétablir les activités prioritaires ainsi que leurs dépendances et ressources de support ; et

c) atténuer, répondre aux impacts et les gérer.

La détermination de la stratégie doit inclure l'approbation des délais de reprise des activités, par ordre de priorité.

L'organisation doit réaliser des évaluations de la capacité de continuité d'activité des fournisseurs.

8.3.2 Etablissement des exigences concernant les ressources

L'organisation doit déterminer les exigences concernant les ressources pour mettre en œuvre les stratégies choisies. Les types de ressources considérés doivent comprendre, sans toutefois s'y limiter :

a) les personnes ;

b) les informations et les données ;

c) les bâtiments, l'environnement de travail et les utilités associées ;

d) les installations, les équipements et les consommables ;

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

f) le transport ;

g) le financement ; et

h) les partenaires et fournisseurs.

8.3.3 Protection et atténuation

Pour les risques identifiés nécessitant un traitement, l'organisation doit envisager des mesures proactives qui :

a) réduisent la probabilité de perturbation ;

b) réduisent la durée de la perturbation ; et

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

L'organisation doit choisir et mettre en œuvre des traitements du risque appropriés en fonction de son appétence au risque.

8.4 Etablissement et mise en œuvre de procédures de continuité d'activité

8.4.1 Généralités

L'organisation doit établir, mettre en œuvre et tenir à jour des procédures de continuité d'activité lui permettant de gérer un incident perturbateur et de poursuivre ses activités, selon les objectifs de reprise identifiés lors de l'analyse des impacts sur l'activité.

L'organisation doit documenter les procédures (y compris les dispositions nécessaires) lui permettant d'assurer la continuité des activités et le management d'un incident perturbateur.

Les procédures doivent :

a) établir un protocole de communications internes et externes approprié ;

b) être précis concernant les mesures immédiates devant être prises pendant une perturbation ;

c) être souples pour répondre à des menaces non prévues et à des conditions internes et externes variables ;

d) se concentrer sur l'impact d'événements pouvant potentiellement perturber les opérations ;

e) être développées sur la base d'hypothèses établies et d'une analyse des interdépendances ; et

f) être efficaces dans la réduction des conséquences par la mise en œuvre de stratégies d'atténuation appropriées.

8.4.2 Structure de réponse à un incident

L'organisation doit établir, documenter et mettre en œuvre des procédures et une structure de management lui permettant de répondre à un incident perturbateur en faisant appel à un personnel ayant les responsabilités, l'autorité et les compétences nécessaires pour gérer l'incident.

La structure de réponse doit :

a) identifier les seuils d'impact justifiant le déclenchement d'une réponse formelle ;

b) évaluer la nature et l'étendue d'un incident perturbateur ainsi que son impact potentiel ;

c) activer une réponse appropriée en termes de continuité d'activité ;

d) disposer de processus et de procédures pour l'activation, le fonctionnement, la coordination et la communication de la réponse ;

e) disposer des ressources disponibles pour soutenir les processus et les procédures de gestion d'un incident perturbateur afin d'en réduire au minimum l'impact ; et

f) communiquer avec les parties intéressées et les autorités ainsi qu'avec les médias.

En considérant la sécurité des personnes comme la première priorité et en consultation avec les parties intéressées concernées, l'organisation doit décider de communiquer ou non, en externe, sur ces risques et impacts significatifs et étayer sa décision par des documents. Si l'organisation décide de communiquer, elle doit alors établir et mettre en œuvre des procédures pour cette communication externe, des alertes et des avertissements auprès des médias si besoin.

8.4.3 Avertissement et communication

L'organisation doit définir, mettre en œuvre et tenir à jour des procédures pour :

a) détecter l'incident ;

b) surveiller régulièrement l'incident ;

c) gérer la communication interne au sein de l'organisation et la réception, la documentation et la réponse à une communication émanant des parties intéressées ;

d) gérer la réception, la documentation et la réponse à un système consultatif national ou régional sur les risques ou un système équivalent ;

e) garantir la disponibilité des moyens de communication au cours d'un incident perturbateur ;

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

g) effectuer l'enregistrement des informations critiques concernant l'incident, les actions entreprises et les décisions prises, et les éléments suivants doivent également être considérés et mis en œuvre lorsque cela est approprié :

— l'alerte des parties intéressées potentiellement touchées par un incident perturbateur réel ou imminent ;

— l'assurance de l'interopérabilité des multiples services d'urgence et le personnel de l'organisation ;

— le fonctionnement d'une installation de communication.

Les procédures de communication et d'avertissement doivent faire l'objet d'exercices réguliers.

8.4.4 Plans de continuité d'activité

L'organisation doit établir des procédures documentées lui permettant de répondre à un incident perturbateur et de poursuivre ou rétablir ses activités dans un délai prédéterminé. De telles procédures doivent concerner les exigences applicables à ceux qui les utiliseront.

Les plans de continuité d'activité doivent généralement contenir :

a) les rôles et les responsabilités définis des personnes et des équipes ayant autorité pendant et après un incident ;

b) un processus d'activation de la réponse ;

c) les détails permettant de gérer les conséquences immédiates d'un incident perturbateur en tenant dûment compte

   1) du bien-être des individus ;

   2) des options stratégiques, tactiques et opérationnelles pour répondre à la perturbation ; et

   3) de la prévention de toute perte ou indisponibilité supplémentaire d'activités prioritaires ;

d) les détails concernant la manière et les circonstances dans lesquelles l'organisation communiquera avec les employés et leurs proches, les parties intéressées clés et les personnes à contacter en cas d'urgence ;

e) la manière dont l'organisation poursuivra ou reprendra ses activités prioritaires dans les délais prédéterminés ;

f) les détails de la réponse de l'organisation aux médias à la suite d'un incident, y compris :

   1) une stratégie de communication ;

   2) l'interface préférée avec les médias ;

   3) des lignes directrices ou un modèle de rédaction d'une déclaration pour les médias ; et

   4) des porte-parole appropriés ;

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

Chaque plan doit définir :

— le but et le domaine d'application ;

— les objectifs ;

— les critères et les procédures d'activation ;

— les procédures de mise en œuvre ;

— les rôles, les responsabilités et les autorités ;

— les exigences et les procédures de communication ;

— les interdépendances et interactions internes et externes ;

— les exigences en termes de ressources ; et

— les processus relatifs au flux d'information et à la documentation.

8.4.5 Reprise

L'organisation doit disposer de procédures documentées lui permettant de rétablir et de reprendre ses activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident.

8.5 Exercices et tests

L'organisation doit procéder à des exercices et des tests de ses procédures de continuité d'activité afin de s'assurer qu'elles sont cohérentes avec ses objectifs de continuité d'activité.

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

a) sont cohérents avec le périmètre et les objectifs du SMCA ;

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

c) cumulés au fil du temps, valident l'ensemble de ses dispositions en matière de continuité d'activité, en impliquant les parties concernées ;

d) minimisent le risque de perturbation des opérations ;

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

f) sont revus dans le cadre d'une promotion de l'amélioration continue ; et

g) sont menés à des intervalles planifiés et lorsque des changements significatifs interviennent au sein de l'organisation ou dans l'environnement dans lequel elle opère.

9 Evaluation des performances

9.1 Supervision, mesurage, analyse et évaluation

9.1.1 Généralités

L'organisation doit déterminer :

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

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

c) quand la surveillance et la mesure doivent être effectuées ; et

d) quand les résultats de la surveillance et de la mesure doivent être analysés et évalués.

L'organisation doit conserver des informations documentées pertinentes comme preuves des résultats.

L'organisation doit évaluer les performances du SMCA, ainsi que l'efficacité du SMCA.

En outre, l'organisation doit :

— agir, lorsque cela est nécessaire, pour remédier aux évolutions ou résultats négatifs avant l'apparition d'une non-conformité ;

— conserver des informations documentées appropriées comme preuves des résultats.

Les procédures de supervision des performances doivent prévoir :

— d'établir des mesures de performances adaptées aux besoins de l'organisation ;

— de surveiller dans quelle mesure la politique, les objectifs et les cibles de continuité d'activité de l'organisation sont respectés/atteints ;

— les performances des processus, des procédures et des fonctions qui protègent ses activités prioritaires ;

— de surveiller la conformité à la présente Norme internationale et aux objectifs de continuité d'activité ;

— de surveiller les preuves historiques de performances insuffisantes du SMCA ; et

— d'enregistrer les données et les résultats de la surveillance et des mesures pour faciliter les actions correctives ultérieures.

NOTE Les performances insuffisantes peuvent comprendre une non-conformité, des quasi-accidents, des fausses alertes et des incidents réels.

9.1.2 Evaluation des procédures de continuité d'activité

a) L'organisation doit mener des évaluations de ses procédures et de ses capacités en matière de continuité d'activité pour s'assurer qu'elles demeurent pertinentes, adéquates et efficaces ;

b) ces évaluations doivent être réalisées par le biais de revues périodiques, d'exercices, de tests, de rapports post-incident et d'évaluations des performances. Les changements significatifs intervenus doivent être pris en compte en temps opportun dans la ou les procédures ;

c) l'organisation doit évaluer périodiquement la conformité aux exigences légales et réglementaires applicables, aux meilleures pratiques de son secteur ainsi que la conformité à sa propre politique de continuité d'activité et aux objectifs associés ; et

d) l'organisation doit mener des évaluations à des intervalles planifiés et lorsque des changements significatifs interviennent.

Lorsqu'un incident perturbateur se produit et entraîne l'activation de ses procédures de continuité d'activité, l'organisation doit procéder à une revue après l'incident et enregistrer les résultats.

9.2 Audit interne

L'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management de la continuité d'activité.

a) est conforme :

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

   2) aux exigences de la présente Norme internationale ; et

b) est efficacement mis en œuvre et tenu à jour.

L'organisation doit :

— planifier, établir, mettre en œuvre et tenir à jour un (des) programme(s) d'audit, couvrant notamment la fréquence, les méthodes, les responsabilités, les exigences de planification et de comptes-rendus. Le(s) programme(s) d'audit doi(ven)t tenir compte de l'importance des processus concernés et des résultats des audits précédents,

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

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

— s'assurer qu'il est rendu compte des résultats des audits à la Direction concernée ; et

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

Le programme d'audit, quel que soit le moment où il est conduit, doit reposer sur les résultats des évaluations du risque des activités de l'organisation et sur les résultats des audits précédents. Les procédures d'audit doivent englober le périmètre, la fréquence, les méthodologies et les compétences, ainsi que les responsabilités et les exigences applicables à la conduite des audits et à la rédaction d'un rapport présentant les résultats.

Le management responsable du domaine audité doit assurer que toutes les corrections et actions correctives nécessaires sont entreprises sans délai indu pour éliminer les non-conformités détectées et leurs causes. Les actions de suivi doivent inclure la vérification des actions entreprises et le compte-rendu des résultats de cette vérification.

9.3 Revue de direction

A des intervalles planifiés, la Direction doit procéder à la révision du SMCA de l'organisation, à des intervalles planifiés afin de s'assurer qu'il est toujours approprié, adapté et efficace.

La revue de Direction doit prendre en compte :

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

b) les modifications des enjeux externes et internes pertinents pour le système de management de la continuité d'activité ;

c) les informations sur les performances en matière 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 supervision et du mesurage ; et

   3) les résultats des audits ;

d) les axes d'amélioration continue.

Les revues de direction doivent prendre en compte les performances de l'organisation, y compris :

— le suivi des actions décidées lors des revues de direction précédentes ;

— la nécessité d'apporter des modifications au SMCA, y compris la politique et les objectifs ;

— les axes d'amélioration ;

— les résultats des audits et des révisions du SMCA, y compris ceux des fournisseurs et partenaires clés le cas échéant ;

— les techniques, les produits ou les procédures, qui pourraient être utilisés dans l'organisation pour améliorer les performances et l'efficacité du SMCA ;

— l'état d'avancement des actions correctives ;

— les résultats des exercices et des tests ;

— les risques ou les questions qui n'ont pas été traités de manière appropriée lors d'une précédente évaluation des risques ;

— tous les changements pouvant affecter le SMCA, qu'ils soient internes ou externes au périmètre du SMCA ;

— l'adéquation de la politique ;

— les recommandations d'amélioration ;

— les leçons tirées et les actions découlant d'incidents perturbateurs ; et

— les bonnes pratiques et lignes directrices qui apparaissent.

Les conclusions de la revue de direction doivent inclure les décisions relatives aux axes d'amélioration continue et aux éventuels changements nécessaires à apporter au SMCA, et comprendre les éléments suivants :

a) les variations apportées au périmètre du SMCA ;

b) l'amélioration de l'efficacité du SMCA ;

c) la mise à jour de l'évaluation des risques, du bilan d'impact sur les activités, des plans de continuité d'activité et des procédures associées ;

d) la modification des procédures et des contrôles pour répondre à des événements internes ou externes qui peuvent influer sur le SMCA, y compris les changements apportés aux :

   1) exigences métier et opérationnelles ;
   2) exigences de réduction des risques et de sécurité ;
   3) conditions et processus opérationnels ;
   4) exigences légales et réglementaires ;
   5) obligations contractuelles ;
   6) niveaux de risque et/ou critères d'acceptation des risques,
   7) besoins en termes de ressources ;
   8) exigences en matière de financement et de budget ; et

e) la manière dont l'efficacité des contrôles est mesurée.

L'organisation doit conserver des informations documentées attestant des conclusions des revues de direction.

L'organisation doit :

— communiquer les conclusions de la revue de direction aux parties intéressées concernées ; et

— entreprendre l'action appropriée en relation avec ces conclusions.

10 Amélioration

10.1 Non-conformité et actions correctives

Lorsqu'une non-conformité se produit, l'organisation doit

a) identifier la non-conformité ;

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

   1) agir pour la maîtriser et la corriger ; et

   2) faire face aux conséquences ;

c) évaluer s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité, de sorte qu'elles ne se reproduisent pas, au même endroit ou ailleurs, en :

   1) révisant la non-conformité ;

   2) déterminant les causes de la non-conformité ; et

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

   4) évaluant le besoin d'entreprendre des actions correctives pour s'assurer que les non-conformités ne se reproduisent pas, au même endroit ou ailleurs ;

   5) déterminant et mettant en œuvre les actions correctives nécessaires ;

   6) révisant l'efficacité de toute action corrective mise en œuvre ; et

   7) modifiant, si nécessaire, le SMCA ;

d) mettre en œuvre toutes les actions nécessaires ;

e) réviser l'efficacité de toute action corrective mise en œuvre ;

f) modifier, si nécessaire, le système de management de la continuité d'activité.

Les actions correctives doivent être à la mesure des effets des non-conformités rencontrées.

L'organisation doit conserver des informations documentées comme preuves :

— de la nature des non-conformités et de toute action subséquente ; et

— des résultats de toute action corrective.

10.2 Amélioration continue

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du SMCA.

NOTE L'organisation peut utiliser les processus du SMCA tels que le leadership, la planification et l'évaluation des performances, afin d'aboutir à 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/CEI 20000-1, *Technologies de l'information — Gestion des services.*

[5] ISO 22300, *Sécurité sociétale — Terminologie.*

[6] ISO/PAS 22399, *Sécurité sociétale — Lignes directrices pour être préparé à un incident et gestion de continuité opérationnelle.*

[7] ISO/CEI 24762, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour les services de secours en cas de catastrophe dans les technologies de l'information et des communications.*

[8] ISO/CEI 27001, *Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité de l'information — Exigences.*

[9] ISO/CEI 27031, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires.*

[10] ISO 31000, *Management du risque — Principes et lignes directrices.*

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

[12] ISO/CEI Guide 73, *Management du risque — Vocabulaire.*

[13] BS 25999-1, *Business continuity management — Code of practice*, British Standards Institution (BSI)

[14] BS 25999-2, *Business continuity management — Specification*, British Standards Institution (BSI)

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

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

[17] *Business Continuity Plan Drafting Guideline*, Ministry of Economy, Trade and Industry (Japan), 2005

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

[19] ANSI/ASIS SPC.1, *Organizational Resilience: Security, Preparedness, and Continuity Managements Systems – Requirements with Guidance for Use*SS 540: 2008, *Singapore Standard for Business Continuity Managemen*t

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