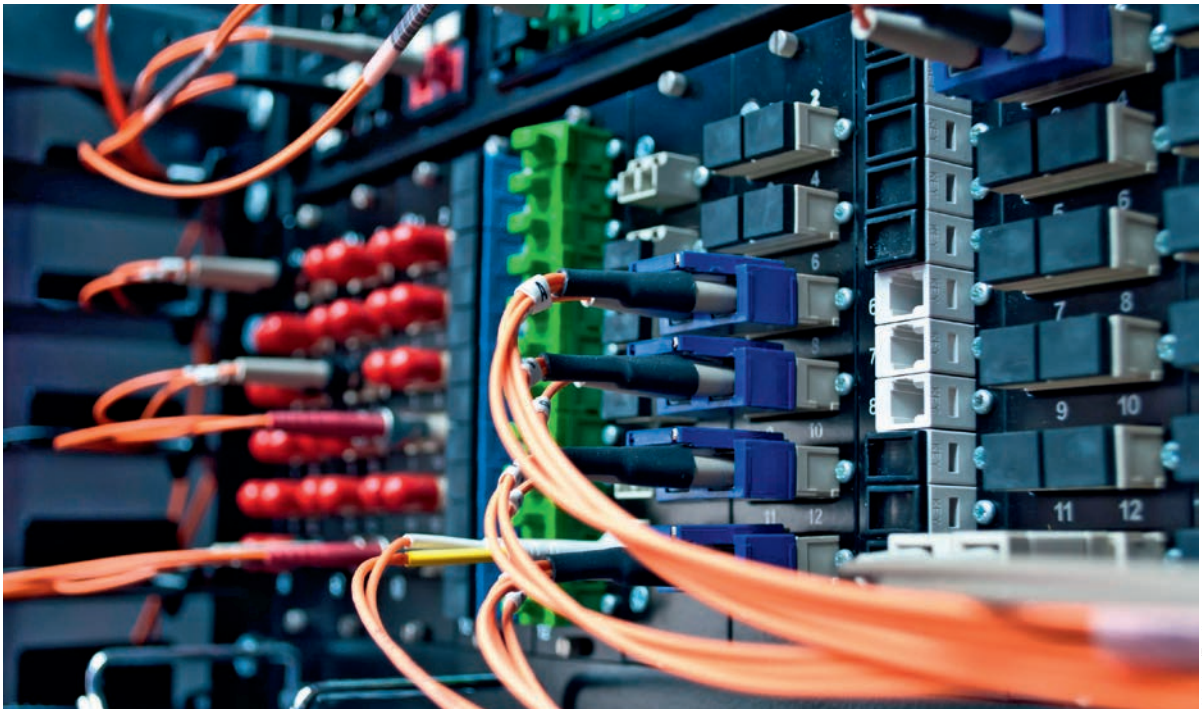
La norme ISO 22301, pour aller mieux quand tout va mal

Publiée en juin 2012, la norme internationale ISO 22301, Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences, devrait permettre à toute organisation, quelle que soit sa taille ou son secteur d'activité, de structurer sa résilience face aux événements non souhaités.



Les systèmes d'information sont une nouvelle vulnérabilité des organisations. Après une crise, il faut assurer la continuité des flux. ▶

Aleksandrs/Fotolia.com

La multiplication et la complexité des crises, l'évolution permanente des organisations, l'augmentation et la globalisation des échanges, les dépendances croissantes aux technologies contribuent à créer des environnements de plus en plus instables pouvant mettre en difficulté les organisations publiques et privées. Face à ces réalités, l'ISO a ouvert un nouveau comité technique traitant de la sécurité sociétale, c'est-à-dire la sécurité en général dans la société, le TC 223. Ce dernier a développé un recueil de normes dont le porte-drapeau est la norme ISO 22301. Cette nouvelle norme internationale sur les Systèmes de management de la continuité d'activité (SMCA) a été publiée en juin 2012.

La continuité des activités prépare les organisations à réagir face à une crise majeure et à préserver leurs activités coeur de leur métier en cas de survenance. La continuité est un outil stratégique de gestion des risques qui contribue à la résilience (capacité à rebondir à la suite d'une crise) des organisations et plus largement à la sécurité sociétale.

Jusque-là, les référentiels normatifs ou de bonnes pratiques en continuité des activités reposaient souvent sur la BS 25999 « *Requirements for Business Continuity Management System* » et sur les guides de bonnes pratiques publiés par des organismes spécialisés tels le DRII et la NFPA américains et le BCI britannique.

La continuité des activités doit mobiliser l'ensemble des acteurs métiers et fonctions supports (im-

mobilier, moyens généraux, DSI, RH, communication, juridique, etc), et tous les niveaux de l'organisation, décisionnels et opérationnels. Elle implique également les parties prenantes, tels que les actionnaires, autorités de tutelle, partenaires, fournisseurs, prestataires et clients.
En France, la continuité des activités reste souvent axée sur les ressources supports, particulièrement le système d'information. Dans les pays de culture anglo-saxonne, de nombreuses organisations ont intégré la continuité à leur programme de gestion des risques, synonyme de maturité.

La continuité des activités peut devenir un avantage concurrentiel

Selon plusieurs études, dont celles du Gartner et de Marsh, les principales difficultés rencontrées pour développer la continuité des activités au sein des organisations sont un manque de compréhension, des difficultés à prioriser, ou encore des écarts entre ressources allouées et ressources nécessaires.
Les « leviers » ou facteurs moteurs pour y remédier restent les bonnes pratiques, les retours d'expériences et la conformité réglementaire. La continuité est cependant de plus en plus considérée comme un avantage concurrentiel et l'ISO 22301 intervient alors que les organisations commencent à percevoir que leur business peut être amélioré grâce à la continuité.
La norme permet aux organisations d'avoir une démarche structurée et reconnue, elle fournit un cadre de référence en matière de SMCA et spécifie formellement un ensemble d'exigences. Celles-ci portent sur la conception, le développement, la mise en œuvre et le maintien en conditions opérationnelles dans une logique d'amélioration continue (cycle PDCA). Comme toute norme de système de management, l'ISO 22301 est auditable et peut aboutir à l'obtention d'une certification.
Ses exigences sont génériques et s'adressent à toutes les organisations (ou parties de celles-ci), indépendamment de leur type, de leur taille ou de leur nature.
Elles sont traitées dans les chapitres 4 à 10 de la norme. Le chapitre 8 « Opérations » traite des processus spécifiques à la continuité des activités tels que l'analyse des impacts métier (BIA), l'appréciation des risques, la définition des stratégies de continuité, le développement et la mise en œuvre des réponses et plans, ainsi que la conduite de tests et exercices. Les autres chapitres reprennent les exigences relatives au système de management semblables


Atmospheric/Fotolia.com

◀ **La continuité des activités doit mobiliser l'ensemble des acteurs métiers mais également les fonctions supports.**

UNE NORME ET DES GUIDES

L'ISO 22301 est une norme de système de management qui spécifie des exigences, mais ne précise pas la manière dont on doit s'organiser. Des guides pratiques la complètent :

> ISO 22300 qui spécifie le vocabulaire de la continuité d'activité.

> ISO 22313, guide de mise en œuvre d'un SMCA conforme à la 22301. Il suit les mêmes chapitres et en précise les exigences, avec des compléments opérationnels intéressants. Néanmoins, il demeure largement insuffisant pour mettre en œuvre un SMCA, ne permet pas une mise en œuvre séquentielle de la norme, ni de distinguer les actions projet et récurrentes, les processus composant le SMCA nécessitent d'être définis selon l'organisation, etc.

> ISO 27031, guide de mise en œuvre de la Préparation des technologies de l'information et de communication à la continuité d'activité (PTCA), composante du SMCA, assimilable au Plan de secours informatique (PSI). Il contient des recommandations en matière d'organisation, de processus, de ressources et moyens de secours nécessaires pour satisfaire aux exigences de continuité métiers et garantir un niveau de résilience des infrastructures et systèmes d'information répondant aux stratégies retenues. Publiée en 2011, la 27031 s'intègre très bien dans chacun des processus du SMCA, notamment en partant du principe qu'une analyse d'impact (BIA) doit être réalisée en amont et que la gestion des incidents perturbateurs se décline à l'échelle de l'informatique. Une mise à jour demeure néanmoins indispensable tant son vocabulaire peut paraître abscons (PTCA/IRBC) ou incohérent avec les autres normes ISO en vigueur (ISO 22301, ISO 31000 et 27005).

> ISO 31000, lignes directrices pour le management du risque. L'appréciation des risques est présentée dans la norme ISO 22301 comme une composante indispensable, au même titre que le BIA, pour la définition des stratégies de continuité d'activité. Cette étape, bien souvent négligée en continuité d'activité, impose un arbitrage des incidents perturbateurs par une démarche structurée. L'ISO 31000 donne le cadre générique de toute méthode de gestion des risques. Elle permet d'uniformiser le vocabulaire et les activités en management du risque favorisant ainsi l'harmonisation et la comparaison entre les secteurs d'activités et les techniques d'appréciation des risques. Volontairement imprécise, elle laisse à chacun la liberté de s'appuyer sur les méthodes respectant un cadre générique fixé, comme par exemple l'ISO 27005. Seule, elle est inefficace pour la réalisation concrète d'une appréciation des risques : absence de base de connaissance, imprécisions sur les composantes d'un risque, etc.

Gilles Rolle/REA

Anticiper l'inattendu et faire face aux perturbations des opérations. ▲

AVANTAGES D'UN SMCA CONFORME À L'ISO 22301

Les bénéfices apportés par la mise en place d'un Système de management de la continuité d'activité selon l'ISO 22301 sont nombreux :

> une compréhension améliorée du métier et des fonctions supports de l'organisation (obtenue durant le BIA et l'appréciation des risques) ;

> la protection des actifs physiques et informationnels des métiers ;

> la réactivité et l'efficacité de l'organisation face aux crises : prises de décisions améliorées par la connaissance du risque ;

> la réduction des impacts en cas de crise réelle ;

> le renforcement de la conformité réglementaire ;

> la préservation des marchés par l'assurance d'un SMCA opérant et continu ;

> un apport de confiance aux parties prenantes sur la résilience de l'organisation ;

> une augmentation indirecte du niveau de résilience, grâce au principe d'amélioration continue.

à celles que l'on peut trouver dans un SMQ (qualité) ou un SMSI (systèmes d'information), par exemple la compréhension du contexte, l'engagement de la direction générale, les ressources supports, la surveillance et le ré-examen, la revue de direction, les actions correctives et l'amélioration continue.

L'importance des analyses préalables

Un SMCA conforme à la norme ISO 22301 ne garantit pas nécessairement un haut niveau de résilience de l'organisation, mais simplement que la continuité d'activité est gérée de manière efficace et que le niveau de résilience est en adéquation avec les enjeux métiers. C'est la notion d'amélioration continue du SMCA qui contribue indirectement à augmenter le niveau de résilience en s'alignant avec les objectifs de continuité d'activité fixés par la direction.

La structure de l'ISO 22301 est conforme aux nouvelles lignes directrices de l'ISO/Guide 83 (structure à haut niveau et texte identique pour les normes de systèmes de management, terminologie de base et définitions communes), lui permettant ainsi de s'intégrer facilement aux systèmes de management déjà présents au sein des organisations, tout en respectant une cohérence globale.
À ce sujet, la structure de la norme autour du modèle PDCA (*Plan-Do-Check-Act* - principes de l'amélioration continue selon la roue de Deming) apporte un message très fort : la norme ISO 22301 positionne les phases d'analyses préalables (BIA et Appréciation des risques) dans le chapitre consacré au « Do », les considérant comme aussi importantes que la gestion de crise et l'application des procédures de continuité.
La norme ISO 22301 était également très attendue pour régler le

sempiternel problème de vocabulaire en continuité d'activité. Nous ne pouvons qu'être déçus sur ce point puisque plusieurs termes fondamentaux ne sont pas clairement définis (exercices et tests), voire totalement absent (Plan de reprise d'activité – PRA). Ces imprécisions se justifient certainement par la volonté de correspondre à tout type de contexte et d'éviter de prendre parti entre les approches américaine/anglo-saxonne et les profils continuité/informaticien.

Le gestionnaire des risques dispose d'un rôle important dans la mise en œuvre et l'exploitation d'un SMCA. Il doit travailler en collaboration avec:

• les juristes et les métiers afin de décliner les exigences légales, réglementaires et contractuelles en exigences de continuité d'activité pragmatiques;

• les autres départements de gestion des risques afin d'harmoniser l'appréciation des risques du SMCA avec la ou les méthode(s) de gestion des risques interne(s);

• les métiers afin d'intégrer dans l'appréciation des risques les conséquences identifiées dans le cadre du BIA et les événements redoutés;

• le responsable PCA (RPCA), les métiers et les responsables des fonctions supports pour définir les mesures proactives et les stratégies de continuité, suivre leur mise en œuvre et mettre à jour en conséquence l'appréciation des risques;

• la direction générale pour lui présenter et faire arbitrer les risques d'incidents perturbateurs.

Plusieurs organismes de certification se sont déjà positionnés sur la certification ISO 22301 dont Afnor Certification, BSI et LSTI. Les audits peuvent être commandités par les clients, partenaires, autorités de tutelle pour s'assurer des engagements contractuels pris au titre de la continuité d'activité.

Au-delà de la réponse à une exigence contractuelle ou réglementaire en matière de résilience, la certification ISO 22301 est un nouveau levier d'apport de confiance. Une telle certification procure un avantage concurrentiel lorsque la continuité et la résilience sont des critères décisifs pour le client, elle est aussi un facteur de réduction des exigences en fonds propres et garantie de la solvabilité. ■

Thomas Le Poetvin,
Hervé Schauer
Consultants HSC

STRUCTURE DE LA NORME

Les étapes clé d'une démarche conforme à l'ISO 22301 sont:

> **la compréhension des besoins de l'organisation et des parties prenantes via une approche systémique globale (4.2 et 4.3);**

> **l'implication et l'engagement plein et entier de la direction générale dans le SMCA (5.1 & 5.2);**

> **la définition et la mise en place des moyens et des plans (7, 8.1, 8.3, 8.4) qui sont listés et détaillés dans l'ISO 22313, ainsi que les tests et exercices (8.5);**

> **le développement de la culture de la continuité au sein de l'organisation (7.2 à 7.4);**

> **l'évaluation de la performance des moyens mis en œuvre et de l'efficacité du SMCA (9);**

> **l'amélioration continue dans la durée (10).**

LES SIGLES DE LA CONTINUITÉ D'ACTIVITÉ

> **BCI: *Business Continuity Institute***

> **BIA: *Business Impact Analysis* - Analyse des impacts ou conséquences sur les métiers**

> **CRBF: Comité de la réglementation bancaire et financière. Les principaux articles du règlement concernant la continuité sont les articles 4, 14, 37 et 39**

> **DNS: Directives nationales de sécurité - exigences émises par le SGDN (Secrétariat général à la défense nationale) à destination des OIV (Opérateurs d'importance vitale), visant à renforcer la protection des infrastructures stratégiques en établissant une politique de sécurité commune aux services de l'État et aux entreprises.**

> **DRII: *Disaster Recovery Institute International***

> **EPCIP: *European Program for Critical Infrastructure Protection***

> **ICT: *Information and Communications Technology***

> **IRBC: *Information and Communications Technology Readiness for Business Continuity***

> **MIFID: *Markets in Financial Instruments Directive***

> **NFPA: *National Fire Protection Association* (www.nfpa.org). Référentiels disponibles en français auprès du CNPP: www.cnpp.com/fr/Boutique-Editions/Referentiels/Referentiels-NFPA**

> **OCDE: Organisation pour la coopération et le développement économique (www.oecd.org)**

> **PDCA: *Plan Do Check Act* - Cycle d'amélioration continue**

> **RPCA: Responsable du plan de continuité des activités**

> **SAIV: Secteur d'activité d'importance vitale. 12 SAIV définis par arrêté du 2 juin 2006, regroupent les opérateurs d'importance vitale.**

> **SMQ: Système de management de la qualité**

> **SMSI: Système de management de la sécurité de l'information (ISO 27001)**