La continuité d'activité a sa norme ISO

Ce 15 mai, l'organisation ISO annonce le lancement de la **norme ISO 22301,** ***« Sécurité sociétale – Systèmes de Gestion de la Continuité des Activités – Exigences »***. Il s'agit d'un international de management, au même titre que ceux sur la sécurité ou sur la qualité. Cette norme va mettre aux oubliettes le seul « standard » existant en la matière, la norme britannique BS25999.

La France est longtemps restée le parent pauvre en normes de continuité, domaine où le pragmatisme anglo-saxon a pris de l'avance. Ainsi les premières formations certifiantes se faisaient sous l'égide du british standard et d'organismes anglais ou québécois. La nouvelle norme spécifie formellement un ensemble d'exigences pour déployer, mettre en œuvre et améliorer en permanence un système de gestion de la continuité de l'activité (SMCA) menant à une certification.

Les exigences spécifiées dans la norme ISO 22301 sont génériques et prévues pour s'appliquer à toutes les organisations (ou parties de celles-ci), indépendamment du type, de la taille et de la nature de l'organisation.

Dans un récent document de synthèse, le cabinet d'études Duquesne Group constate au moins deux bonnes raisons de s'intéresser à cette certification :

- son adoption par l'entreprise indique clairement une intention d'amélioration inscrite dans la durée en matière de continuité ;
- les partenaires de l'entreprise – clients ou fournisseurs – savent que des mesures sont en place et que l'entreprise présente un niveau de risque et un degré de préparation face au sinistre meilleurs que d'autres.

L'enjeu, expliquent les analystes, c'est de se rapprocher le plus possible d'un « état cible ». Donc, il faut raisonner en termes d'amélioration de la situation, usant de bonnes pratiques. Et non pas s'attendre à y trouver des recettes toutes faites. Pour en comprendre l'esprit, on peut faire l'analogie avec les normes de sécurité ISO 27000 ou celles plus connues encore sur la qualité (ISO 9000). C'est une approche « système de management » – qui, au passage, requiert l'adhésion explicite de la direction générale – souligne le cabinet Duquesne.

Mettre en place une politique de continuité

Il faut donc, idéalement, commencer par élaborer un document de « politique de continuité ». Cette démarche s'apparente exactement à celle décrite par les « qualiticiens » et la roue de Deming, comme « PDCA » : plan (planifier), do (réaliser,concrétiser), check (contrôler, vérifier) et act (réagir, corriger). Mais attention, c'est une norme qui spécifie clairement des choses à faire obligatoirement : 'you shall' en anglais, en plus des bonnes pratiques recommandées ('you should').

Les consultants du cabinet Duquesne comparent également l'approche britannique, très orientée BIA (business impact analysis) et celle des États-Unis (priorité à l'analyse de risques). La norme réconcilie tout le monde en demandant les deux, dans l'ordre que l'on veut.

La norme énumère un certain nombre de recommandations et de critères – à commencer par la

nomination d'un manager responsable « PCA ». Ce qui signifie la reconnaissance d'une qualification. D'où l'apparition – logique – de formations agréées qui certifient les stagiaires.

Dans un premier temps, il faut mettre en place le système de management du PCA, c'est pour cela que les premières certifications sont de type 'lead implementer'. Ensuite il faudra auditer ce qui a été fait, des certifications 'lead auditor' ISO 22301 apparaîtront dans ce but.

Certification et formation agréées

Comme pour les normes ISO 9000 et ISO 27001 il existe deux types de certification : une pour les personnes (où l'on certifie une acquisition de compétence) et une autre pour les sociétés où l'on certifie une réalisation concrète.

Ainsi, il faut procéder dans l'ordre : l'entreprise recourt autant que possible à des 'implementers' certifiés (des individus) pour mettre en place son PCA et peut alors se faire auditer (par des auditeurs certifiés) pour obtenir son certificat (d'entreprise). Il est courant d'ailleurs en France que l'entreprise se contente de former et certifier ses principaux intervenants en PCA (implementers et auditors), sans rechercher le certificat final pour elle-même (ainsi, par exemple en ISO 27001, il y a des milliers de gens formés et certifiés ISO ; il y a fort peu d'entreprises certifiées… une vingtaine ?).

En France, le seul organisme français délivrant des certifications 'lead implementer' est LSTI qui a agréé pour cela Duquesne Group. En effet, celui qui certifie un stagiaire ne peut être celui qui forme : l'ISO l'exige ainsi. La certification ISO 22301 'lead implementer' est accordée par le Laboratoire LSTI de Saint-Malo, cofondé par Armelle Trotin (ingénieur en sécurité SI, ancien officier de la Marine française) et Philippe Bouchet, ingénieur télécoms (vice président de la Commission Nationale Sécurité SI au sein de l'Afnor).

Le cabinet Duquesne Group a été la première organisation a obtenir de LSTI, en mars 2012, l'agrément de formateur ISO 22301. Il peut donc dispenser des formations d »implementer' de la norme 22301 auprès de chefs de projet chargés de mettre en place des systèmes de management de la continuité d'activité conformes à cette norme.