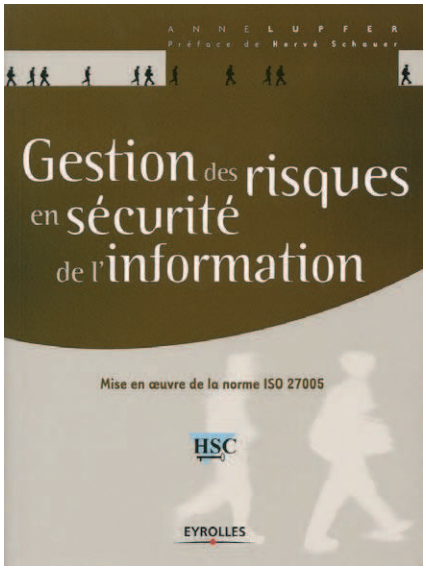
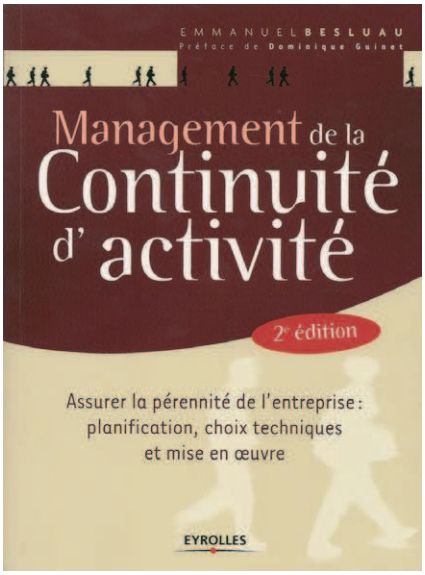
Les bonnes pratiques de la sécurité

Par Laurence Essirart



Gestion des risques en sécurité de l'information, mise en œuvre de la norme ISO 27005,
par Anne Lupfer,
Eyrolles, 229 pages.



Management de la continuité d'activité, assurer la pérennité de l'entreprise : planification, choix techniques et mise en œuvre,
par Emmanuel Besluau,
deuxième édition, Eyrolles, 298 pages.

La norme ISO 27005 n'est pas un référentiel à proprement parler. Il s'agit, selon Anne Lupfer, responsable sécurité d'un grand groupe, d'un « *guide de mise en œuvre qui donne des lignes directrices qu'il convient de suivre, d'adapter et parfois d'ignorer dans la conception, le développement et l'exploitation de son système de gestion de risques.* » La norme ISO 27005, après les démarches locales (par exemple Méhari en France, développée par le Clusif) constitue « *la première méthode de gestion des risques structurée et normalisée, appelée à s'imposer à l'échelle planétaire* », résume l'auteur. Le processus de gestion de risques se modélise en six étapes : l'établissement du contexte, l'identification du risque, son estimation, son évaluation, son traitement et son acceptation. Le processus est itératif, avec la surveillance et le réexamen des risques.

« *Grâce à l'application d'un modèle d'amélioration continue et du principe itératif sur le processus de gestion des risques, l'entreprise peut augmenter progressivement son niveau de maîtrise des risques* », assure l'auteur. La première étape est qualifiée de « *primordiale* » et souvent absente des méthodes de gestion des risques les plus classiques. L'estimation des risques peut être rapide si l'on suit les recommandations de la norme : « *Sinon, elle pourra être particulièrement fastidieuse* », assure l'auteur. L'évaluation du risque est, elle, souvent source de discussions, voire de désaccords, alors qu'elle conditionne le traitement des risques. Le choix de celui-ci « *nécessite d'analyser la situation et de se projeter dans le futur* », en considérant des éléments tels que les coûts immédiats, les conséquences pour l'organisation, l'adhésion des utilisateurs, la stratégie de l'entreprise. L'ouvrage présente des études de cas : celui d'un grand groupe international qui met en place une nouvelle méthode de gestion de risques, celui d'une mairie d'une ville de 50 000 habitants souhaitant renforcer la sécurité de son système d'information et celui d'un organisme bancaire implanté en France et à l'international.

La seconde édition de l'ouvrage d'Emmanuel Besluau sur la continuité d'activité, s'intéresse à un sujet qui, selon l'auteur, « *n'a pas actuellement en France l'attention qu'il mérite de la part des directions générales.* » Dans les faits « *focalisée sur des analyses de risques théoriques, l'entreprise néglige souvent l'impact réel des sinistres potentiels et ne connaît pas les processus les plus critiques* ». Avec une « *confiance exagérée dans une technologie fragile et une défiance désabusée pour les dispositifs d'organisation utiles* », ajoute l'auteur, consultant associé chez Duquesne Group.

L'ouvrage s'articule autour de quatre parties. La première est consacrée à la prise de conscience du risque : comment déterminer les faiblesses de l'entreprise ? Comment limiter l'exposition aux risques et les conséquences ? La deuxième partie décrit comment construire ses équipes, attribuer les missions, organiser les tests et les plannings. Le troisième volet propose un tour d'horizon technologique, avec les différents mécanismes en jeu (serveurs, stockage, architectures, réseaux, postes de travail, infrastructures, *cloud computing*…) et leur retour sur investissement. Enfin, l'auteur aborde la gouvernance pour superviser la mise en œuvre d'un plan de continuité. ◆