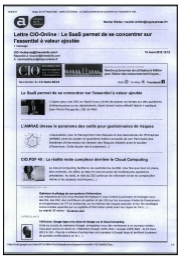
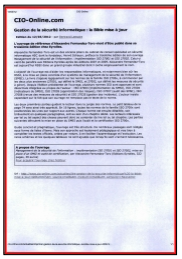
CIO NEWSLETTER
6/8 RUE JEAN JAURES
92800 PUTEAUX - 01 41 97 02 02





14 MARS 12
Parution irrégulière

Surface approx. (cm²) : 175

Gestion de la sécurité informatique : la Bible mise à jour

Edition du 12/03/2012 - par Bertrand Lemaire

L'ouvrage de référence d'Alexandre Fernandez-Toro vient d'être publié dans sa troisième édition chez Eyrolles.

Alexandre Fernandez-Toro est un des anciens piliers du cabinet de conseil spécialisé en sécurité informatique HSC dont le fondateur, Hervé Schauer, préface la troisième édition de son ouvrage *Management de la sécurité de l'information : implémentation ISO 27001 et ISO 27002*. Celui-ci vient de paraître aux Editions Eyrolles après les éditions 2007 et 2009. Alexandre Fernandez-Toro est aujourd'hui RSSI dans un grand groupe industriel dont il cache soigneusement le nom.

L'objectif de l'ouvrage est d'aider les responsables informatiques, et notamment bien sûr les RSSI, à la mise en place concrète d'un système de management de la sécurité de l'information (SMSI). Le livre s'appuie logiquement sur les normes de la famille ISO 2700x, à commencer par les deux plus anciennes (27001, qui définit le SMSI, et 27002, qui définit les mesures de sécurité à gérer). Depuis l'édition précédente de l'ouvrage, plusieurs normes ISO sont apparues et sont désormais intégrées au propos de l'auteur : ISO 27003 (implémentation du SMSI), ISO 27004 (indicateurs du SMSI), ISO 27005 (appréciation des risques), ISO 27007 (audit des SMSI), ISO 27008 (revue des mesures de sécurité) et ISO 27035 (gestion des incidents). L'auteur insiste cependant sur le fait que son ouvrage ne remplace pas le texte de la norme.

Les deux premières parties guident le lecteur dans la jungle des normes. Le petit tableau de la page 74 sera ainsi très apprécié. En 16 lignes, toutes les normes de la famille ISO 2700x sont positionnées les unes par rapport aux autres. Chaque norme est ensuite détaillée, soit brièvement en quelques paragraphes, soit au sein d'un chapitre dédié. Les lecteurs intéressés par tel ou tel aspect des choses peuvent donc se contenter de lire tel ou tel chapitre. Les parties suivantes déroulent la mise en place du SMSI puis l'audit et la certification ISO 2700x.

Guide concret et pragmatique, l'ouvrage est très structuré. De nombreux passages sont rédigés sous forme de listes d'items. Mais son approche est hautement pédagogique et vise bien à compléter les textes officiels, arides par nature, à en faciliter l'apprentissage et l'exécution. Les rares schémas et les quelques tableaux ne sont ajoutés que lorsqu'ils sont vraiment nécessaires.