Livre : Management de la sécurité de l'information

Management de la sécurité de l'information
Par Alexandre Fernandez-Toro

Eyrolles collection HSC – 324 pages – 39 euros TTC

Auditeur de certification et consultant, Alexandre Fernandez-Toro est RSSI d'une grande entreprise française et a longtemps dirigé les activités ISO 27001 d'HSC. Il baigne donc depuis longtemps dans les normes ISO 2700x, ce qui transparait nettement dans cet ouvrage, le lecteur ne s'en plaindra pas.

Le sous-titre de l'ouvrage, *« Implémentation ISO 27001 et ISO 27002, Mise en place d'un SMSI et audit de certification »*, a le mérite d'être très clair. Son objectif est d'accompagner les professionnels, en particulier les RSSI, qui souhaitent d'une part comprendre la norme, et d'autre part mettre en place un SMSI (Système de Management de la Sécurité de l'Information).

Pour cela, l'auteur nous invite tout d'abord à aborder les **systèmes de management**, avant de s'attaquer au gros morceau, les **normes**. Eh oui, *« les normes »*, à commencer par ISO 27001, suivie par ISO 27002. Sur la première, l'accent est mis sur le plan SMSI et ses différentes phases (Do, Check, Act). La seconde bénéficie d'un traitement tourné vers sa présentation et son chapitrage.

Toujours *« les normes »* avec la seconde partie du livre consacrée aux **normes de la série ISO 27000** et à leur implémentation au SMSI. Défilent en autant de chapitres l'implémentation de l'ISO 27003, les indicateurs SMSI ISO 27004, l'appréciation des risques ISO 27005, l'audit des SMSI ISO 27007, la revue des mesures de sécurité ISO 27008, et la gestion des incidents de sécurité ISO 27035.

Implémenter un SMSI

La partie suivante est consacrée à l'**implémentation d'un SMSI**. Elle occupe près de la moitié du livre et sera très appréciée par les RSSI qui souhaitent se lancer dans une démarche de SMSI, tout comme ceux, en particulier les DSI, qui vont l'accompagner. Au fil des chapitres, l'expérience de l'auteur transparaît là encore nettement et sera appréciée. Il évoque le projet, la politique, le périmètre, la gouvernance, la documentation, l'audit interne, l'appréciation des risques, la sélection des mesures de sécurité, la sensibilisation et les indicateurs.

Et de terminer sur une dernière partie non moins importante pour les RSSI qui souhaitent aller jusqu'au bout de leur démarche, l'**audit des SMSI**. Ou peut-être devrions-nous dire *« les audits »*. Une partie relativement courte, mais qui est la bienvenue. Nombre d'ouvrages préparent aux connaissances techniques liées aux démarches de certification, mais combien vont jusqu'à évoquer la préparation et le déroulement de l'audit lui-même ?

Terminons sur le dernier chapitre, qui clôt la dernière partie, qui aurait presque pu servir d'introduction, tant il nous a paru pertinent, car il s'adresse moins aux RSSI qu'à l'entreprise ou au client qui s'interroge sur la démarche. **À quoi sert une certification ISO** pour la sécurité de l'information, comment l'analyser, la comparer, quel est son périmètre ? Autant de questions qui viennent terminer cet ouvrage en forme de bible – le terme est ici parfaitement adapté – qui nous semble bien amenée et suffisamment documentée pour devenir indispensable à tous ceux qui s'intéressent au sujet.